

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2003-115832**

(43)Date of publication of application : **18.04.2003**

(51)Int.Cl. **H04L 9/08**

G06F 12/14

H04L 9/20

H04N 5/44

H04N 5/76

(21)Application number : **2001-307559**

(71)Applicant : **NIPPON HOSO KYOKAI <NHK>**

(22)Date of filing : **03.10.2001**

(72)Inventor : **NISHIMOTO TOMONARI
KURIOKA TATSUYA
UEHARA TOSHIHIRO
NANBA SEIICHI**

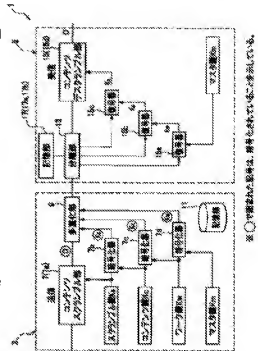
(54) CONTENTS TRANSMITTING DEVICE, CONTENTS RECEIVING DEVICE, CONTENTS TRANSMITTING PROGRAM AND CONTENTS RECEIVING PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method, a device and a program for transmitting/ receiving contents, in which efficiency is improved when descrambling scrambled contents, a cryptographic key is easily managed when descrambling the contents, and the copyright of the contents can be protected.

SOLUTION: A system is composed of a contents transmitting device 3 for enciphering and transmitting contents and a contents receiving device 5 for receiving the contents, the contents transmitting device 3 is provided with a contents scramble part 7 for enciphering the contents by using a scramble key K_s , a contents key K_c , a work key K_w and a master key K_m and a multiplexing part 9 for multiplexing the contents and sending them as multiplex enciphered contents and the contents receiving device 5 is provided

with a demultiplexing part 13 for receiving and demultiplexing the multiplied enciphered contents and a contents descrambler part 15 for obtaining the contents by deciphering enciphered information demultiplexed by the demultiplexing part 13.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-115832

(P2003-115832A)

(43) 公開日 平成15年4月18日 (2003.4.18)

(51) Int. Cl. ⁷	識別記号	F I	テマコード [*] (参考)
H 0 4 L 9/08		G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
G 0 6 F 12/14	3 2 0	H 0 4 N 5/44	Z 5 C 0 2 5
H 0 4 L 9/20		5/76	Z 5 C 0 5 2
H 0 4 N 5/44		H 0 4 L 9/00	6 0 1 B 5 J 1 0 4
5/76			6 0 1 A

審査請求 未請求 請求項の数30 ○L (全 31 頁) 最終頁に続く

(21) 出願番号 特願2001-307559(P2001-307559)

(71) 出願人 000004352

日本放送協会

東京都渋谷区神南2丁目2番1号

(22) 出願日 平成13年10月3日 (2001.10.3)

(72) 発明者 西本 友成

東京都世田谷区砦一丁目10番11号 日本放

送協会放送技術研究所内

(72) 発明者 栗岡 辰弥

東京都世田谷区砦一丁目10番11号 日本放

送協会放送技術研究所内

(74) 代理人 100064414

弁理士 磯野 道造

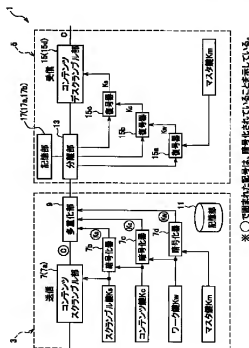
最終頁に続く

(54) 【発明の名称】 コンテンツ送信装置、コンテンツ受信装置およびコンテンツ送信プログラム、コンテンツ受信プログラム

(57) 【要約】

【課題】 スクラブルされたコンテンツをデスクランブルする際の効率を向上させ、デスクランブルする際の暗号鍵の管理を容易にし、コンテンツの著作権を保護できるコンテンツ送信、受信方法とその装置とそのプログラムとを提供する。

【解決手段】 コンテンツを暗号化して送信するコンテンツ送信装置3と受信するコンテンツ受信装置5とからなり、コンテンツ送信装置3が、スクランブル鍵K_s、コンテンツ鍵K_c、ワーク鍵K_w、マスター鍵K_mを用いてコンテンツを暗号化するコンテンツスクランブル部7と、多重化して多重暗号コンテンツとして送出する多重化部9とを備え、コンテンツ受信装置5が多重暗号コンテンツを受信して分離する分離部13と、この分離部13で分離された暗号化された情報を復号してコンテンツを得るコンテンツデスクランブル部15とを備えた。



* 図中○で囲まれた符号は本発明に係る符号を示している。

【特許請求の範囲】

【請求項1】 デジタル放送におけるコンテンツを暗号化して送信するコンテンツ送信装置であって、経過時間と共に変更されるスクランブル鍵と、前記コンテンツ毎に設けられたコンテンツ鍵と、受信側に共通に備えられたマスター鍵とを記憶する記憶手段と、前記スクランブル鍵により、前記コンテンツを暗号化した暗号化コンテンツとするコンテンツ暗号化手段と、前記コンテンツ鍵により、少なくとも前記スクランブル鍵を含む前記コンテンツに関する関連情報を暗号化した暗号化関連情報とする関連情報暗号化手段と、前記マスター鍵により、少なくとも前記コンテンツ鍵を含む当該コンテンツに関する関連情報を暗号化した暗号化コンテンツ鍵関連情報とするコンテンツ鍵関連情報暗号化手段と、

前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、を多重化した多重暗号コンテンツとする多重化手段と、この多重化手段で多重化された多重暗号コンテンツを送信する多重暗号コンテンツ送信手段と、を備えることを特徴とするコンテンツ送信装置。

【請求項2】 デジタル放送におけるコンテンツを暗号化して送信するコンテンツ送信装置であって、経過時間と共に変更されるスクランブル鍵と、前記コンテンツ毎に設けられたコンテンツ鍵と、前記コンテンツの継続時間よりも長時間にわたり保持されるワーク鍵と、受信側に共通に備えられたマスター鍵とを記憶する記憶手段と、前記スクランブル鍵により、前記コンテンツを暗号化した暗号化コンテンツとするコンテンツ暗号化手段と、前記コンテンツ鍵により、少なくとも前記スクランブル鍵を含む前記コンテンツに関する関連情報を暗号化した暗号化関連情報とする関連情報暗号化手段と、前記ワーク鍵により、少なくとも前記コンテンツ鍵を含む当該コンテンツ鍵に関する関連情報を暗号化した暗号化コンテンツ鍵関連情報とするコンテンツ鍵関連情報暗号化手段と、

前記マスター鍵により、少なくとも前記ワーク鍵を含む当該ワーク鍵に関する関連情報を暗号化した暗号化ワーク鍵関連情報とするワーク鍵関連情報暗号化手段と、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報を多重化した多重暗号コンテンツとする多重化手段と、

この多重化手段で多重化された多重暗号コンテンツを送信する多重暗号コンテンツ送信手段と、を備えることを特徴とするコンテンツ送信装置。

【請求項3】 デジタル放送におけるコンテンツを暗号化して送信するコンテンツ送信装置であって、経過時間と共に変更されるスクランブル鍵と、前記コンテンツ毎に設けられたコンテンツ鍵と、前記コンテンツ

の継続時間よりも長時間にわたり保持されるワーク鍵と、受信側に共通に備えられたマスター鍵とを記憶する記憶手段と、

前記スクランブル鍵により、前記コンテンツを暗号化した暗号化コンテンツとするコンテンツ暗号化手段と、前記コンテンツ鍵により、少なくとも前記スクランブル鍵を含む前記コンテンツに関する関連情報を暗号化した暗号化関連情報とする関連情報暗号化手段と、前記ワーク鍵により、少なくとも前記コンテンツ鍵を含む当該コンテンツ鍵に関する関連情報を暗号化した暗号化コンテンツ鍵関連情報とするコンテンツ鍵関連情報暗号化手段と、

前記マスター鍵により、少なくとも前記ワーク鍵を含む当該ワーク鍵に関する関連情報を暗号化した暗号化ワーク鍵関連情報とするワーク鍵関連情報暗号化手段と、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化ワーク鍵関連情報を多重化した多重暗号コンテンツとする多重化手段と、

この多重化手段で多重化された多重暗号コンテンツを送信する多重暗号コンテンツ送信手段と、

前記暗号化コンテンツ鍵関連情報を、前記多重暗号コンテンツの送信開始時刻後の所定の時間、または、前記多重暗号コンテンツの送信を開始する送信開始時刻より所定の時間前から送信終了時刻の所定の時間後まで、所定の時間間隔で繰り返し送信する、或いは、受信側で前記暗号化コンテンツ鍵関連情報を受信していない場合に、受信側からの要求に基づいて送信する若しくは通信回線網を介して送信するか、の少なくとも一つの手段により、前記暗号化コンテンツ鍵関連情報を送信する暗号化コンテンツ鍵関連情報送信手段と、を備えることを特徴とするコンテンツ送信装置。

【請求項4】 受信側で、復号されたコンテンツ鍵関連情報が記憶される、外部より読み出し不可能なセキュリティモジュールが備えられる場合、このセキュリティモジュールが、前記受信側の受信装置に対応するように複数個設けられており、これら複数個のセキュリティモジュールが複数のグループにグループ分けされており、このグループ分けされたセキュリティモジュールのグループ毎に対応する複数の前記ワーク鍵が備えられていることを特徴とする請求項2または請求項3に記載のコンテンツ送信装置。

【請求項5】 受信側で前記暗号化コンテンツ鍵関連情報を復号しコンテンツ鍵関連情報とした後、当該コンテンツ鍵関連情報を、そのまま、或いは別途暗号化して保持する際に、受信側の受信装置が記憶手段、記憶媒体を取り扱う記憶媒体取扱手段の少なくとも一方を備える場合、前記セキュリティモジュール、前記記憶手段、前記記憶媒体のいずれかに当該コンテンツ鍵関連情報を保持させることを指定するコンテンツ鍵関連情報記憶指定手段を備えることを特徴とする請求項4に記載のコンテ

ツ送信装置。

【請求項6】 受信側で記憶媒体を取り扱う記憶媒体取扱手段を備える際に、当該記憶媒体に前記暗号化コンテンツが記憶され、当該暗号化コンテンツが再生されると共に、当該暗号化コンテンツに対応する暗号化コンテンツ鍵関連情報を送信している場合には、当該暗号化コンテンツ鍵関連情報を利用せずに、保持されたコンテンツ鍵関連情報を利用するように指定するコンテンツ鍵関連情報利用指定手段を備えることを特徴とする請求項1から請求項5のいずれか1項に記載のコンテンツ送信装置。

【請求項7】 前記セキュリティモジュール毎に、当該セキュリティモジュールから出力させる情報を暗号化する複数の固有鍵が当該セキュリティモジュール内部に設定されており、これら固有鍵を、前記マスター鍵で暗号化し暗号化固有鍵設定用関連情報とする固有鍵設定用関連情報暗号化手段を備えることを特徴とする請求項4から請求項6のいずれか1項に記載のコンテンツ送信装置。

【請求項8】 前記固有鍵の少なくとも1つが、他のセキュリティモジュールと共通に設定されていることを特徴とする請求項7に記載のコンテンツ送信装置。

【請求項9】 送信側でデジタル放送におけるコンテンツが暗号化され、この暗号化されたコンテンツを受信するコンテンツ受信装置であって、

前記送信側において、経過時間と共に変更されるスクランブル鍵により前記コンテンツが暗号化された暗号化コンテンツと、前記コンテンツ鍵に設けられたコンテンツ鍵により、少なくとも前記スクランブル鍵を含む前記コンテンツに関する関連情報が暗号化された暗号化関連情報と、前記送信側に共通に備えられたマスター鍵により、少なくとも前記コンテンツ鍵を含む当該コンテンツ鍵に関する関連情報が暗号化された暗号化コンテンツ鍵関連情報とが多重化された多重暗号コンテンツが送信され、この多重暗号コンテンツを受信する多重暗号コンテンツ受信手段と、

この多重暗号コンテンツ受信手段で受信した多重暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、に分離する多重暗号コンテンツ分離手段と、

当該暗号化コンテンツ鍵関連情報を前記マスター鍵で復号し、復号されたコンテンツ鍵で前記暗号化関連情報に含まれるスクランブル鍵を復号し、復号されたスクランブル鍵で前記暗号化コンテンツを復号し、前記コンテンツを得る多重暗号コンテンツ復号手段と、を備えることを特徴とするコンテンツ受信装置。

【請求項10】 送信側でデジタル放送におけるコンテンツが暗号化され、この暗号化されたコンテンツを受信するコンテンツ受信装置であって、

ンブル鍵により前記コンテンツが暗号化された暗号化コンテンツと、前記コンテンツ毎に設けられた暗号化コンテンツ鍵により、少なくとも前記スクランブル鍵を含む前記コンテンツに関する関連情報が暗号化された暗号化関連情報と、前記コンテンツの経過時間よりも長時間にわたり保持されるワーク鍵により、少なくとも前記コンテンツ鍵を含む当該コンテンツに関する関連情報が暗号化された暗号化コンテンツ鍵関連情報と、前記送信側に共通に備えられたマスター鍵により、少なくとも前記ワーク鍵を含む当該ワーク鍵に関する関連情報が暗号化された暗号化ワーク鍵関連情報とが多重化された多重暗号コンテンツが送信され、この多重暗号コンテンツを受信する多重暗号コンテンツ受信手段と、

この多重暗号コンテンツ受信手段で受信した多重暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報に分離する多重暗号コンテンツ分離手段と、

当該暗号化ワーク鍵関連情報を前記マスター鍵で復号し、復号されたワーク鍵で前記暗号化コンテンツ鍵関連情報に含まれるコンテンツ鍵を復号し、復号されたコンテンツ鍵で前記暗号化関連情報に含まれるスクランブル鍵を復号し、復号されたスクランブル鍵で前記暗号化コンテンツを復号し、前記コンテンツを得る多重暗号コンテンツ復号手段と、を備えることを特徴とするコンテンツ受信装置。

【請求項11】 前記暗号化コンテンツ鍵関連情報が得られていない場合に、送信側に暗号化コンテンツ鍵関連情報を要求する暗号化コンテンツ鍵関連情報要求手段を備えることを特徴とする請求項9または請求項10に記載のコンテンツ受信装置。

【請求項12】 前記マスター鍵が内部に設定された、外部より読み出し不可能なセキュリティモジュールを備え、復号後のコンテンツ鍵関連情報と、このコンテンツ鍵関連情報に係り、コンテンツを識別するコンテンツ識別子とを前記セキュリティモジュールに記憶するコンテンツ鍵関連情報記憶手段を備えることを特徴とする請求項9から請求項11のいずれか1項に記載のコンテンツ受信装置。

【請求項13】 前記マスター鍵および出力させる情報を暗号化する固有鍵が内部に設定された、外部より読み出し不可能なセキュリティモジュールを備え、復号後のコンテンツ鍵関連情報と、このコンテンツ鍵関連情報に係り、コンテンツを識別するコンテンツ識別子とを前記セキュリティモジュールに記憶するコンテンツ鍵関連情報記憶手段を備えることを特徴とする請求項9から請求項11のいずれか1項に記載のコンテンツ受信装置。

【請求項14】 前記固有鍵の少なくとも1つが、他の

セキュリティモジュールと共通に設定されていることを特徴とする請求項13に記載のコンテンツ受信装置。

【請求項15】 前記固有鍵が複数設けられており、送信側において、前記マスター鍵により、これらの固有鍵が暗号化され、暗号化固有鍵設定用関連情報とされ、この暗号化固有鍵設定用関連情報を受信する暗号化固有鍵設定用関連情報受信手段と、この暗号化固有鍵設定用関連情報受信手段で受信した暗号化固有鍵設定用関連情報をも前記マスター鍵により復号する暗号化固有鍵設定用関連情報復号手段と、を備えることを特徴とする請求項13または請求項14に記載のコンテンツ受信装置。

【請求項16】 前記復号後のコンテンツ鍵関連情報を記憶する場合に、前記セキュリティモジュールのメモリ容量を越えた場合に、当該復号後のコンテンツ鍵関連情報が記憶された時間、送信側または受信側により設定された設定情報に基づいて、当該復号後のコンテンツ鍵関連情報を削除するコンテンツ鍵関連情報削除手段を備えることを特徴とする請求項12から請求項15のいずれか1項に記載のコンテンツ受信装置。

【請求項17】 前記セキュリティモジュールに記憶した前記復号後のコンテンツ鍵関連情報を出力し、記憶するコンテンツ鍵関連情報出力記憶手段を備えることを特徴とする請求項12から請求項16のいずれか1項に記載のコンテンツ受信装置。

【請求項18】 前記復号後のコンテンツ鍵関連情報を記憶する場合に、前記記憶手段のメモリ容量を越えた場合に、当該復号後のコンテンツ鍵関連情報が記憶された時間、送信側または受信側により設定された設定情報に基づいて、当該復号後のコンテンツ鍵関連情報を削除するコンテンツ鍵関連情報削除手段を備えることを特徴とする請求項17に記載のコンテンツ受信装置。

【請求項19】 前記セキュリティモジュールに記憶した前記復号後のコンテンツ鍵関連情報、前記マスター鍵で暗号化し、再暗号化コンテンツ鍵関連情報として出力し、かつ記憶するコンテンツ鍵関連情報再暗号化記憶手段を備えることを特徴とする請求項12から請求項18のいずれか1項に記載のコンテンツ受信装置。

【請求項20】 前記再暗号化コンテンツ鍵関連情報およびコンテンツを識別するコンテンツ識別子が前記記憶手段に記憶され、当該記憶手段のメモリ容量を越えた場合に、当該再暗号化コンテンツ鍵関連情報が記憶された時間、送信側または受信側により設定された設定情報に基づいて、当該再暗号化コンテンツ鍵関連情報を削除する再暗号化コンテンツ鍵関連情報削除手段を備えることを特徴とする請求項19に記載のコンテンツ受信装置。

【請求項21】 前記セキュリティモジュールに記憶した前記復号後のコンテンツ鍵関連情報、前記固有鍵で暗号化し、固有暗号化コンテンツ鍵関連情報として出力し、かつ記憶するコンテンツ鍵関連情報固有暗号化記憶

手段を備えることを特徴とする請求項12から請求項16のいずれか1項に記載のコンテンツ受信装置。

【請求項22】 前記固有暗号化コンテンツ鍵関連情報およびコンテンツを識別するコンテンツ識別子が前記記憶手段に記憶され、当該記憶手段のメモリ容量を越えた場合に、当該固有暗号化コンテンツ鍵関連情報が記憶された時間、送信側または受信側により設定された設定情報に基づいて、当該固有暗号化コンテンツ鍵関連情報を削除する固有暗号化コンテンツ鍵関連情報削除手段を備えることを特徴とする請求項21に記載のコンテンツ受信装置。

【請求項23】 前記復号後のコンテンツ鍵関連情報を、前記マスター鍵で再暗号化した再暗号化コンテンツ鍵関連情報とし、この再暗号化コンテンツ鍵関連情報に対応する暗号化コンテンツと共に、記憶媒体に記憶する記憶媒体取扱手段を備えることを特徴とする請求項9から請求項15のいずれか1項に記載のコンテンツ受信装置。

【請求項24】 前記復号後のコンテンツ鍵関連情報を、前記固有鍵で再暗号化した固有暗号化コンテンツ鍵関連情報として、この固有暗号化コンテンツ鍵関連情報に対応する暗号化コンテンツと共に、記憶媒体に記憶する記憶媒体取扱手段を備えることを特徴とする請求項13から請求項15のいずれか1項に記載のコンテンツ受信装置。

【請求項25】 記憶手段および記憶媒体取扱手段を備え、この記憶媒体取扱手段によって取り扱われる記憶媒体に、前記スクランブル鍵で暗号化された暗号化コンテンツと、この暗号化コンテンツを識別するコンテンツ識別子を含む前記コンテンツに関する暗号化関連情報とを記憶させるための暗号化コンテンツ記憶手段と、前記記憶媒体に記憶された前記暗号化コンテンツを再生する際に、当該暗号化コンテンツに対応する再暗号化コンテンツ鍵関連情報か前記記憶手段、前記記憶媒体の少なくともも一方に記憶されている場合、当該再暗号化コンテンツ鍵関連情報を前記記憶手段または前記記憶媒体から読み出して、前記セキュリティモジュールに入力すると共に、前記暗号化関連情報を入力する関連情報入力手段と、

前記マスター鍵により、前記再暗号化コンテンツ鍵関連情報を復号し、コンテンツ鍵を得、このコンテンツ鍵により、前記暗号化関連情報を復号し、スクランブル鍵を得、このスクランブル鍵を出力するスクランブル鍵出力手段と、

このスクランブル鍵出力手段で出力されたスクランブル鍵で、前記記憶媒体の暗号化コンテンツを復号する暗号化コンテンツ復号手段と、を備えることを特徴とする請求項12から請求項16および請求項19、請求項20、請求項23のいずれか1項に記載のコンテンツ受信装置。

【請求項26】 記憶手段および記憶媒体取扱手段を備え、この記憶媒体取扱手段によって取り扱われる記憶媒体に、前記スクランブル鍵で暗号化された暗号化コンテンツと、この暗号化コンテンツを識別するコンテンツ識別子を含む前記コンテンツに関する暗号化関連情報とを記憶させるための暗号化コンテンツ記憶手段と、

前記記憶媒体に記憶された前記暗号化コンテンツを再生する際に、当該暗号化コンテンツに対応する固有暗号化コンテンツ鍵関連情報が前記記憶手段、前記記憶媒体の少なくとも一方に記憶されている場合、当該固有暗号化コンテンツ関連情報を前記記憶手段または前記記憶媒体から読み出して、前記セキュリティモジュールに入力すると共に、前記暗号化関連情報を入力する関連情報入力手段と、

前記固有鍵により、前記固有暗号化コンテンツ鍵関連情報を復号し、コンテンツ鍵を得、このコンテンツ鍵により、前記暗号化関連情報を復号し、スクランブル鍵を得、このスクランブル鍵を出力するスクランブル鍵出力手段と、

このスクランブル鍵出力手段で出力されたスクランブル鍵で、前記記憶媒体の暗号化コンテンツを復号する暗号化コンテンツ復号手段と、を備えることを特徴とする請求項13から請求項16および請求項21、請求項22、請求項24のいずれか1項に記載のコンテンツ受信装置。

【請求項27】 前記暗号化コンテンツを送信中に、当該暗号化コンテンツを記憶しなかった場合、当該暗号化コンテンツに対応するコンテンツ鍵を記憶しないコンテンツ鍵不記憶手段を備えることを特徴とする請求項9から請求項26のいずれか1項に記載のコンテンツ受信装置。

【請求項28】 前記暗号化関連情報を、コンテンツ鍵で復号するタイミングで、当該暗号化関連情報に対応するコンテンツの送信開始時刻、終了時刻に基づいて、当該コンテンツ鍵を切り替えるコンテンツ鍵切替手段を備えることを特徴とする請求項9から請求項27のいずれか1項に記載のコンテンツ受信装置。

【請求項29】 デジタル放送におけるコンテンツを暗号化して送信するコンテンツ送信装置を、

経過時間と共に変更されるスクランブル鍵と、前記コンテンツ毎に設けられたコンテンツ鍵と、前記コンテンツの継続時間より長時間にわたり割り当てられるワーク鍵と、受信側に共通に備えられたマスター鍵とを記憶する記憶手段、

前記スクランブル鍵により、前記コンテンツを暗号化した暗号化コンテンツとするコンテンツ暗号化手段、

前記コンテンツ鍵により、少なくとも前記スクランブル鍵を含む前記コンテンツに関する関連情報を暗号化した暗号化関連情報とする関連情報暗号化手段と、

前記ワーク鍵により、少なくとも前記コンテンツ鍵を含

む当該コンテンツ鍵に関する関連情報を暗号化した暗号化コンテンツ鍵関連情報とするコンテンツ鍵関連情報暗号化手段、

前記マスター鍵により、少なくとも前記ワーク鍵を含む当該ワーク鍵に関する関連情報を暗号化した暗号化ワーク鍵関連情報とするワーク鍵関連情報暗号化手段、

前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報を多重化した多重暗号コンテンツとする多重化手段、

10 この多重化手段で多重化された多重暗号コンテンツを送信する多重暗号コンテンツ送信手段、として機能させることを特徴とするコンテンツ送信プログラム。

【請求項30】 送信側でデジタル放送におけるコンテンツが暗号化され、この暗号化されたコンテンツを受信するコンテンツ受信装置を、

前記送信側に共通に備えられたマスター鍵を記憶する記憶手段、

前記送信側において、経過時間と共に変更されるスクランブル鍵により前記コンテンツが暗号化された暗号化コ

20 ンテンツと、前記コンテンツ毎に設けられたコンテンツ鍵により、少なくとも前記スクランブル鍵を含む前記コンテンツに関する関連情報が暗号化された暗号化関連情報と、前記コンテンツの継続時間より長時間にわたり保持されるワーク鍵により、少なくとも前記コンテンツ

鍵を含む当該コンテンツに関する関連情報が暗号化された暗号化コンテンツ鍵関連情報と、前記マスター鍵により、

少なくとも前記ワーク鍵を含む当該ワーク鍵に関する関連情報が暗号化された暗号化ワーク鍵関連情報とが

30 多重化された多重暗号コンテンツが送信され、この多重暗号コンテンツを受信する多重暗号コンテンツ受信手段、

この多重暗号コンテンツ受信手段で受信した多重暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記ワーク鍵関連情報に分離する多重暗号コンテンツ分離手段、

当該暗号化ワーク鍵関連情報を前記マスター鍵で復号し、復号されたワーク鍵で前記暗号化コンテンツ鍵関連

情報に含まれるコンテンツ鍵を復号し、復号されたコン

テンツ鍵で前記暗号化関連情報に含まれるスクランブル

40 鍵を復号し、復号されたスクランブル鍵で前記暗号化コンテンツを復号し前記コンテンツを得る多重暗号コンテンツ復号手段、として機能させることを特徴とするコンテンツ受信プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタル放送におけるコンテンツを暗号化して、限定した受信者に送信し、受信者側で復号して視聴するコンテンツ送信方法、受信方法およびコンテンツ送信装置、受信装置ならびにコンテンツ送信プログラム、受信プログラムに関する。

【0002】

【従来の技術】従来、デジタル放送における番組（コンテンツ）を放送局側（送信側）で暗号化し、限定した受信者（受信側）に視聴させる、いわゆる限定受信方式では、実時間で放送される暗号化されたコンテンツを復号可能にする装置（受信装置）を所有することが一般的である。

【0003】ここで、従来の限定受信方式の基本構成について、図12を参照して説明する。番組（コンテンツ）信号をスクランブルする方法として、日本の衛星デジタル放送では、ブロック暗号方式が採用されている。このブロック暗号方式は、図12に示すように、短時間（一秒程度）で変更されるスクランブル鍵（Ks）を用い、コンテンツをスクランブル（暗号化）し、長期間（半年から一年程度）で変更されるワーク鍵（Kw）を用い、スクランブル鍵およびコンテンツに関するコンテンツ情報を暗号化しECM（暗号化関連情報）とし、さらに送信側の放送装置および受信側の受信装置に保持される共通のマスター鍵（Km）を用い、ワーク鍵および各受信装置との契約内容を示す情報を暗号化しEMM（個別関連情報）とし、これらを多重化し放送（送信）する方式である。

【0004】また、この多重化された放送を受信する受信側では、多重化された放送を、EMM（個別関連情報）、暗号化されたワーク鍵を含む、ECM（暗号化関連情報）、暗号化されたスクランブル鍵を含む、暗号化されたコンテンツに分離する。そして、送信側の放送装置が保持する共通のマスター鍵により、EMMが復号され、ワーク鍵が得られ、このワーク鍵により、ECMが復号され、スクランブル鍵が得られ、このスクランブル鍵により、暗号化されたコンテンツが復号され、コンテンツが得られる。復号されたコンテンツは場合によって蓄積装置に蓄積される。

【0005】つまり、コンテンツをスクランブルする際に、前記したスクランブル鍵が用いられ、このスクランブル鍵を得られる特定の受信装置を所有する限定した受信者のみ（放送局（放送事業者）と契約を交わした者）がスクランブルされたコンテンツをデスクランブルして視聴することができる。このため、特定の受信装置を所有していない不正受信者（放送局（放送事業者）と契約を交わしていない者）は、スクランブル鍵によるスクランブルを容易に解除することができず、スクランブルされたコンテンツを視聴することができない。つまり、不正にコンテンツを視聴できず、不正視聴に対する安全性が高められている。

【0006】以上、図12を参照して限定受信方式の原理について概略を説明したが、具体的には、例えば、電波産業会（ARIB）の標準規格「デジタル放送における限定受信方式」（ARIB STD-B25）に基づいた方式がある。

【0007】

【発明が解決しようとする課題】そして、近年、受信装置に備えられている記憶装置の大容量化、操作性の向上に伴い、デジタル放送におけるコンテンツを選択して記憶させるのではなく、つまり、従来のようにコンテンツ毎に録画予約をして（取捨選択して）記憶させるのではなく、例えば、ある放送局で放送された数十時間分のコンテンツを一律に記憶させ、記憶後、視聴するコンテンツを選択するといった視聴の仕方が広まりつつある。

【0008】この場合、記憶されるコンテンツの中に、有料コンテンツが含まれている際に、視聴するまでの段階で、この有料コンテンツ（コンテンツ信号）に施されているスクランブル（暗号化）をデスクランブル（復号）する必要がある。そして、有料コンテンツを視聴する視聴者に対し、当該有料コンテンツを視聴した場合に適正な課金を行いたい（適正に課金されたい）という要請がある。すなわち、視聴者は放送された有料コンテンツを記憶しても視聴しない場合があり、有料コンテンツを視聴した時点で課金する、しかしながら、従来の方式では、デスクランブルした状態（スクランブルが解かれた状態）で蓄積すると、実際には、視聴していないのに、課金されてしまうという事態が生じる。そこで、視聴する時に、つまり、記憶媒体等から読み出した時に、デスクランブル処理する方法が考えられている。

【0009】しかし、受信側では、デジタル信号で生成され、暗号化されているコンテンツを記憶する場合、コンテンツ単位、ファイル単位で記憶するのが一般的である。当然のことながら、暗号化されたコンテンツ、ファイル等をデスクランブル処理する時には、このコンテンツ単位、ファイル単位で行われることが効率がよい。しかし、従来の一般的なデスクランブル処理は、ストリーム単位で行われている。このため、デスクランブル処理の効率が悪いという問題がある。

【0010】さらに、コンテンツ単位、ファイル単位でデスクランブル処理を行おうとすると、ストリーム単位でデスクランブル処理を行う場合と比較して、暗号化および復号に用いられる鍵の数が極めて多くなり、これらの鍵を管理することが困難になるという問題がある。またさらに、受信装置にコンテンツが記憶された場合の、当該コンテンツの著作権が保護されないという問題がある。

【0011】本発明の目的は前記した従来の技術が有する課題を解消し、スクランブルされたコンテンツをデスクランブルする際の効率を向上させ、デスクランブルする際の暗号鍵の管理を容易にし、コンテンツの著作権を保護できるコンテンツ送信方法、受信方法およびコンテンツ送信装置、受信装置ならびにコンテンツ送信プログラム、受信プログラムを提供することにある。

【0012】

【課題を解決するための手段】前記した目的を達成する

ため、請求項1記載のコンテンツ送信装置は、デジタル放送におけるコンテンツを暗号化して送信するコンテンツ送信装置であって、経過時間と共に変更されるスクランブル鍵と、前記コンテンツ毎に設けられたコンテンツ鍵と、受信側に共通に備えられたマスター鍵とを記憶する記憶手段と、前記スクランブル鍵により、前記コンテンツを暗号化し暗号化コンテンツとするコンテンツ暗号化手段と、前記コンテンツ鍵により、少なくとも前記スクランブル鍵を含む前記コンテンツに関する関連情報を暗号化し暗号化関連情報とする関連情報暗号化手段と、前記マスター鍵により、少なくとも前記コンテンツ鍵を含む前記コンテンツ鍵に関する関連情報を暗号化し暗号化コンテンツ鍵に関する関連情報暗号化手段と、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵に関する関連情報とを多重化し多重暗号コンテンツとする多重化手段と、この多重化手段で多重化された多重暗号コンテンツを送信する多重暗号コンテンツ送信手段と、を備えることを特徴とする。

【0013】かかる構成によれば、まず、送信されるコンテンツが経過時間と共に変更されるスクランブル鍵によって暗号化され、暗号化コンテンツとされる。そして、スクランブル鍵もコンテンツ毎に設けられたコンテンツ鍵によって、コンテンツに関する関連情報と共に、暗号化され、暗号化関連情報とされる。また、コンテンツ鍵も受信側に共通に備えられたマスター鍵によって、コンテンツ鍵に関する関連情報と共に、暗号化され、暗号化コンテンツ鍵関連情報とされる。その後、暗号化されたこれらの情報が多重化され、送信される。

【0014】なお、コンテンツに関する関連情報とは、送信側（放送事業者）の認証番号（事業者ID）、コンテンツを識別するコンテンツ識別子（コンテンツID）等のことである。また、コンテンツ鍵に関する関連情報とは、送信側（放送事業者）の認証番号（事業者ID）、コンテンツを識別するコンテンツ識別子（コンテンツID）、ワーク鍵を識別するワーク鍵識別子（ワーク鍵ID）等のことである。

【0015】また、請求項2記載のコンテンツ送信装置は、デジタル放送におけるコンテンツを暗号化して送信するコンテンツ送信装置であって、経過時間と共に変更されるスクランブル鍵と、前記コンテンツ毎に設けられたコンテンツ鍵と、前記コンテンツの継続時間よりも長時間にわたり保持されるワーク鍵と、受信側に共通に備えられたマスター鍵とを記憶する記憶手段と、前記スクランブル鍵により、前記コンテンツを暗号化し暗号化コンテンツとするコンテンツ暗号化手段と、前記コンテンツ鍵により、少なくとも前記スクランブル鍵を含む前記コンテンツに関する関連情報を暗号化し暗号化関連情報とする関連情報暗号化手段と、前記ワーク鍵により、少なくとも前記コンテンツ鍵を含む当該コンテンツ鍵に関する関連情報を暗号化し暗号化コンテンツ鍵に関する関連情報暗号化手段と、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵に関する関連情報とを多重化し多重暗号コンテンツとする多重化手段と、この多重化手段で多重化された多重暗号コンテンツを送

するコンテンツ鍵関連情報暗号化手段と、前記マスター鍵により、少なくとも前記ワーク鍵を含む当該ワーク鍵に関する関連情報を暗号化し暗号化ワーク鍵関連情報とするワーク鍵関連情報暗号化手段と、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵に関する関連情報、暗号化ワーク鍵関連情報を多重化し多重暗号コンテンツとする多重化手段と、この多重化手段で多重化された多重暗号コンテンツを送信する多重暗号コンテンツ送信手段と、を備えることを特徴とする。

10 【0016】かかる構成によれば、まず、送信されるコンテンツが経過時間と共に変更されるスクランブル鍵によって暗号化され、暗号化コンテンツとされる。そして、スクランブル鍵もコンテンツ毎に設けられたコンテンツ鍵によって、コンテンツに関する関連情報と共に、暗号化され、暗号化関連情報とされる。また、コンテンツ鍵もコンテンツの継続時間よりも長時間にわたり保持されるワーク鍵によって、コンテンツ鍵に関する関連情報と共に、暗号化され、暗号化コンテンツ鍵関連情報とされる。さらに、ワーク鍵も受信側に共通に備えられたマスター鍵によって、ワーク鍵に関する関連情報と共に、暗号化され、暗号化ワーク鍵関連情報とされる。その後、暗号化されたこれらの情報が多重化され、送信される。

【0017】なお、ワーク鍵に関する関連情報とは、送信側（放送事業者）の認証番号（事業者ID）、受信側に備えられているICカード形態のセキュリティモジュールを識別するセキュリティモジュール識別子（カードID）、更新番号、有効期限、ワーク鍵を識別するワーク鍵識別子（ワーク鍵ID）等のことである。

30 【0018】また、請求項3記載のコンテンツ送信装置は、デジタル放送におけるコンテンツを暗号化して送信するコンテンツ送信装置であって、経過時間と共に変更されるスクランブル鍵と、前記コンテンツ毎に設けられたコンテンツ鍵と、前記コンテンツの継続時間よりも長時間にわたり保持されるワーク鍵と、受信側に共通に備えられたマスター鍵とを記憶する記憶手段と、前記スクランブル鍵により、前記コンテンツを暗号化し暗号化コンテンツとするコンテンツ暗号化手段と、前記コンテンツ鍵により、少なくとも前記スクランブル鍵を含む前記コンテンツに関する関連情報を暗号化し暗号化関連情報とする関連情報暗号化手段と、前記ワーク鍵により、少なくとも前記コンテンツ鍵を含む当該コンテンツ鍵に関する関連情報を暗号化し暗号化コンテンツ鍵に関する関連情報暗号化手段と、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化ワーク鍵関連情報を多重化し多重暗号コンテンツとする多重化手段と、この多重化手段で多重化された多重暗号コンテンツを送

信する多重暗号コンテンツ送信手段と、前記暗号化コンテンツ鍵関連情報を、前記多重暗号コンテンツの送信開始時刻後の所定の時間、または、前記多重暗号コンテンツの送信を開始する送信開始時刻より所定の時間前から送信終了時刻の所定の時間後まで、所定の時間間隔で繰り返し送信する、或いは、受信側で前記暗号化コンテンツ鍵関連情報を受信していない場合に、受信側からの要求に基づいて送信する若しくは通信回線網を介して送信するか、の少なくとも一つの手段により、前記暗号化コンテンツ鍵関連情報を送信する暗号化コンテンツ鍵関連情報送信手段と、を備えることを特徴とする。

【0019】かかる構成によれば、まず、送信されるコンテンツが経過時間と共に変更されるスクランブル鍵によって暗号化され、暗号化コンテンツとされる。そして、スクランブル鍵もコンテンツ毎に設けられたコンテンツ鍵によって、コンテンツに関する関連情報と共に、暗号化され、暗号化関連情報とされる。また、コンテンツ鍵もコンテンツの継続時間よりも長時間にわたり保持されるワーク鍵によって、コンテンツ鍵に関する関連情報と共に、暗号化され、暗号化コンテンツ鍵関連情報とされる。さらに、ワーク鍵も受信側に共通に備えられたマスター鍵によって、ワーク鍵に関する関連情報と共に、暗号化され、暗号化ワーク鍵関連情報とされる。そして、暗号化されたこれらの情報のうち、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報が多重化された多重暗号コンテンツとして送信される。その後、暗号化コンテンツ鍵関連情報送信手段によって、暗号化コンテンツ鍵関連情報が、多重暗号コンテンツの送信開始時刻後の所定の時間、または、前記多重暗号コンテンツの送信を開始する送信開始時刻より所定の時間前から送信終了時刻の所定の時間後まで、所定の時間間隔で繰り返し送信されるか、或いは、受信側からの要求に基づいて送信されるか、または通信回線網を介して送信される。

【0020】また、請求項4記載のコンテンツ送信装置は、請求項2または請求項3に記載のコンテンツ送信装置において、受信側で、復号されたコンテンツ鍵関連情報が記憶される、外部より読み出し不可能なセキュリティモジュールが備えられる場合、このセキュリティモジュールが、前記受信側の受信装置に対応するように複数個設けられており、これら複数個のセキュリティモジュールが複数のグループにグループ分けされており、このグループ分けされたセキュリティモジュールのグループ毎に対応する複数の前記ワーク鍵が備えられていることを特徴とする。

【0021】かかる構成によれば、受信側にセキュリティモジュールが備えられた場合、このセキュリティモジュールがグループ分けされており、このグループ分けされたグループ毎に対応するワーク鍵が備えられる。

【0022】また、請求項5記載のコンテンツ送信装置

は、請求項4に記載のコンテンツ送信装置において、受信側で前記暗号化コンテンツ鍵関連情報を復号しコンテンツ鍵関連情報とした後、当該コンテンツ鍵関連情報を、そのまま、或いは別途暗号化して保持する際に、受信側の受信装置が記憶手段、記憶媒体を取り扱う記憶媒体取扱手段の少なくとも一方を備える場合、前記セキュリティモジュール、前記記憶手段、前記記憶媒体のいずれかに当該コンテンツ鍵関連情報を保持させることを指定するコンテンツ鍵関連情報記憶指定手段を備えることを特徴とする。

【0023】かかる構成によれば、コンテンツ鍵関連情報記憶指定手段によって、受信側でコンテンツ鍵関連情報を保持する場所が、セキュリティモジュール、記憶手段、記憶媒体のいずれかに指定される。

【0024】また、請求項6記載のコンテンツ送信装置は、請求項1から請求項5のいずれか1項に記載のコンテンツ送信装置において、受信側で記憶媒体を取り扱う記憶媒体取扱手段を備える際に、当該記憶媒体に前記暗号化コンテンツが記憶され、当該暗号化コンテンツが再生されるときに、当該暗号化コンテンツに対応する暗号化コンテンツ鍵関連情報を送信している場合には、当該暗号化コンテンツ鍵関連情報を利用して、保持されたコンテンツ鍵関連情報を利用するように指定するコンテンツ鍵関連情報利用指定手段を備えることを特徴とする。

【0025】かかる構成によれば、受信側で、暗号化コンテンツが再生されるときに、コンテンツ鍵関連情報利用指定手段によって、当該暗号化コンテンツを復号するスクランブル鍵に対応するコンテンツ鍵を含むコンテンツ鍵関連情報が送信されている場合であっても、これを利用せずに、保持されているコンテンツ鍵関連情報しか利用できないように指定される。

【0026】また、請求項7記載のコンテンツ送信装置は、請求項4から請求項6のいずれか1項に記載のコンテンツ送信装置において、前記セキュリティモジュール毎に、当該セキュリティモジュールから出力される情報を暗号化する複数の固有鍵が当該セキュリティモジュール内部に設定されており、これら固有鍵を、前記マスター鍵で暗号化した暗号固有鍵設定用関連情報とすると固有鍵設定用関連情報暗号化手段を備えることを特徴とする。

【0027】かかる構成によれば、受信側にセキュリティモジュールが備えられる際に、このセキュリティモジュールの内部に設定される固有鍵が、送信側の固有鍵設定用関連情報暗号化手段によって、マスター鍵により暗号化された暗号固有鍵設定用関連情報とされ、送信される。なお、受信側では、セキュリティモジュールに備えられたマスター鍵によって、暗号化固有鍵設定用関連情報が復号され、固有鍵が得られる。

【0028】また、請求項8記載のコンテンツ送信装置

は、請求項7に記載のコンテンツ送信装置において、前記固有鍵の少なくとも1つが、他のセキュリティモジュールと共通に設定されていることを特徴とする。かかる構成によれば、受信側の他のセキュリティモジュールに共通する固有鍵が設定されているので、この共通の固有鍵を利用すれば、一方のセキュリティモジュールに記憶されている情報（例えば、コンテンツ鍵関連情報）を、他方のセキュリティモジュールで出力させられる。

【0029】さらに、請求項9記載のコンテンツ受信装置は、送信側でデジタル放送におけるコンテンツが暗号化され、この暗号化されたコンテンツを受信するコンテンツ受信装置であって、前記送信側において、経過時間と共に変更されるスクランブル鍵により前記コンテンツが暗号化された暗号化コンテンツと、前記コンテンツ毎に設けられたコンテンツ鍵により、少なくとも前記スクランブル鍵を含む前記コンテンツに関する関連情報が暗号化された暗号化関連情報と、前記送信側に通に備えられたマスター鍵により、少なくとも前記コンテンツ鍵を含む当該コンテンツ鍵に関する関連情報が暗号化された暗号化コンテンツ鍵関連情報とが多重化された多重暗号コンテンツが送信され、この多重暗号コンテンツを受信する多重暗号コンテンツ受信手段と、この多重暗号コンテンツ受信手段で受信した多重暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、に分離する多重暗号コンテンツ分離手段と、当該暗号化コンテンツ鍵関連情報を前記マスター鍵で復号し、復号されたコンテンツ鍵で前記暗号化関連情報に含まれるスクランブル鍵を復号し、復号されたスクランブル鍵で前記暗号化コンテンツを復号し、前記コンテンツを得る多重暗号コンテンツ復号手段と、を備えることを特徴とする。

【0030】かかる構成によれば、まず、送信側で多重された多重暗号コンテンツが、多重暗号コンテンツ受信手段によって、受信される。そして、受信された多重暗号コンテンツは、多重暗号コンテンツ分離手段によって、暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報に分離される。その後、多重暗号コンテンツ復号手段によって、マスター鍵により暗号化コンテンツ鍵関連情報が復号され、コンテンツ鍵が得られ、このコンテンツにより暗号化関連情報が復号され、スクランブル鍵が得られ、このスクランブル鍵により暗号化コンテンツが復号され、コンテンツが得られる。

【0031】また、請求項10記載のコンテンツ受信装置は、送信側でデジタル放送におけるコンテンツが暗号化され、この暗号化されたコンテンツを受信するコンテンツ受信装置であって、前記送信側において、経過時間と共に変更されるスクランブル鍵により前記コンテンツが暗号化された暗号化コンテンツと、前記コンテンツ毎に設けられたコンテンツ鍵により、少なくとも前記スクランブル鍵を含む前記コンテンツに関する関連情報が暗

号化された暗号化関連情報と、前記コンテンツの経過時間よりも長時間にわたり保持されるワーク鍵により、少なくとも前記コンテンツ鍵を含む当該コンテンツに関する関連情報が暗号化された暗号化コンテンツ鍵関連情報と、前記送信側に通に備えられたマスター鍵により、少なくとも前記ワーク鍵を含む当該ワーク鍵に関する関連情報が暗号化された暗号化ワーク鍵関連情報とが多重化された多重暗号コンテンツが送信され、この多重暗号コンテンツを受信する多重暗号コンテンツ受信手段と、この多重暗号コンテンツ受信手段で受信した多重暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報に分離する多重暗号コンテンツ分離手段と、当該暗号化ワーク鍵関連情報を前記マスター鍵で復号し、復号されたワーク鍵で前記暗号化コンテンツ鍵関連情報に含まれるコンテンツ鍵を復号し、復号されたコンテンツ鍵で前記暗号化関連情報に含まれるスクランブル鍵を復号し、復号されたスクランブル鍵で前記暗号化コンテンツを復号し、前記コンテンツを得る多重暗号コンテンツ復号手段と、を備えることを特徴とする。

【0032】かかる構成によれば、まず、送信側で多重された多重暗号コンテンツが、多重暗号コンテンツ受信手段によって、受信される。そして、受信された多重暗号コンテンツは、多重暗号コンテンツ分離手段によって、暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報に分離される。その後、多重暗号コンテンツ復号手段によって、マスター鍵により暗号化ワーク鍵関連情報が復号され、ワーク鍵が得られ、このワーク鍵により暗号化コンテンツ鍵関連情報が復号され、コンテンツ鍵が得られ、このコンテンツにより暗号化関連情報が復号され、コンテンツが得られる。

【0033】また、請求項11記載のコンテンツ受信装置は、請求項9または請求項10に記載のコンテンツ受信装置において、前記暗号化コンテンツ鍵関連情報が得られていない場合に、送信側に暗号化コンテンツ鍵関連情報を要求する暗号化コンテンツ鍵関連情報要求手段を備えることを特徴とする。

【0034】かかる構成によれば、暗号化コンテンツ鍵関連情報が、多重暗号コンテンツに多重化されていない場合、つまり、暗号化コンテンツ鍵関連情報が別途に送信された場合であり、なおかつ、暗号化コンテンツ鍵関連情報が得られていない場合に、暗号化コンテンツ鍵関連情報要求手段によって、送信側にコンテンツ鍵が含まれている暗号化コンテンツ鍵関連情報が要求される。

【0035】また、請求項12記載のコンテンツ受信装置は、請求項9から請求項11のいずれか1項に記載のコンテンツ受信装置において、前記マスター鍵が内部に設定された、外部より読み出し不可能なセキュリティモ

ジュールを備え、復号後のコンテンツ鍵関連情報と、このコンテンツ鍵関連情報に係り、コンテンツを識別するコンテンツ識別子とを前記セキュリティモジュールに記憶するコンテンツ鍵関連情報記憶手段を備えることを特徴とする。

【0036】かかる構成によれば、コンテンツ鍵関連情報記憶手段によって、復号後のコンテンツ鍵関連情報とコンテンツを識別するコンテンツ識別子とが、マスター鍵が設定されたセキュリティモジュールに記憶される。

【0037】また、請求項13記載のコンテンツ受信装置は、請求項9から請求項11のいずれか1項に記載のコンテンツ受信装置において、前記マスター鍵および出力させる情報を暗号化する固有鍵が内部に設定された、外部より読み出し不可能なセキュリティモジュールを備え、復号後のコンテンツ鍵関連情報と、このコンテンツ鍵関連情報に係り、コンテンツを識別するコンテンツ識別子とを前記セキュリティモジュールに記憶するコンテンツ鍵関連情報記憶手段を備えることを特徴とする。

【0038】かかる構成によれば、コンテンツ鍵関連情報記憶手段によって、復号後のコンテンツ鍵関連情報とコンテンツを識別するコンテンツ識別子とが、マスター鍵および固有鍵が設定されたセキュリティモジュールに記憶される。

【0039】また、請求項14記載のコンテンツ受信装置は、請求項13に記載のコンテンツ受信装置において、前記固有鍵の少なくとも1つが、他のセキュリティモジュールと共通に設定されていることを特徴とする。

【0040】かかる構成によれば、マスター鍵および固有鍵が設定されるセキュリティモジュールにおいて、少なくとも1つの固有鍵が、他のセキュリティモジュールと共通に設定されており、この共通の固有鍵を利用すれば、一方のセキュリティモジュールに記憶されている情報（例えば、コンテンツ鍵関連情報）を、他方のセキュリティモジュールで出力され得る。

【0041】また、請求項15記載のコンテンツ受信装置は、請求項13または請求項14に記載のコンテンツ受信装置において、前記固有鍵が複数設けられており、送信側において、前記マスター鍵によって、これらの固有鍵が暗号化され、暗号化固有鍵設定用関連情報とされ、この暗号化固有鍵設定用関連情報を受信する暗号化固有鍵設定用関連情報受信手段と、この暗号化固有鍵設定用関連情報受信手段で受信した暗号化固有鍵設定用関連情報を前記マスター鍵により復号する暗号化固有鍵設定用関連情報復号手段とを、備えることを特徴とする。

【0042】かかる構成によれば、セキュリティモジュールの内部に固有鍵が設定される場合に、暗号化固有鍵設定用関連情報受信手段によって、送信側でマスター鍵により暗号化された暗号化固有鍵設定用関連情報を受信し、暗号化固有鍵設定用関連情報復号手段によって、暗号化固有鍵設定用関連情報を復号し、固有鍵が得られ

る。

【0043】また、請求項16記載のコンテンツ受信装置は、請求項12から請求項15のいずれか1項に記載のコンテンツ受信装置において、前記復号後のコンテンツ鍵関連情報を記憶する場合に、前記セキュリティモジュールのメモリ容量を越えた場合に、当該復号後のコンテンツ鍵関連情報が記憶された時間、送信側または受信側により設定された設定情報に基づいて、当該復号後のコンテンツ鍵関連情報を削除するコンテンツ鍵関連情報削除手段を備えることを特徴とする。

【0044】かかる構成によれば、セキュリティモジュールのメモリ容量を越えた場合に、コンテンツ鍵関連情報削除手段によって、コンテンツ鍵関連情報が記憶された時間、送信側または受信側により設定された設定情報に基づいて、コンテンツ鍵関連情報が削除される。例えば、コンテンツ鍵関連情報が数十時間前に記憶され、長時間経過した場合であっても、受信側で設定した設定情報（当該コンテンツ鍵関連情報はコンテンツを視聴するまで削除しない）を優先させた場合、より優先度合いの低いコンテンツ鍵関連情報の方が速く削除される。

【0045】また、請求項17記載のコンテンツ受信装置は、請求項12から請求項16のいずれか1項に記載のコンテンツ受信装置において、前記セキュリティモジュールに記憶した前記復号後のコンテンツ鍵関連情報を出し、記憶するコンテンツ鍵関連情報出力記憶手段を備えることを特徴とする。

【0046】かかる構成によれば、セキュリティモジュールに記憶された復号後のコンテンツ鍵関連情報が、コンテンツ鍵関連情報出力記憶手段によって、出力され記憶される。

【0047】また、請求項18記載のコンテンツ受信装置は、請求項17に記載のコンテンツ受信装置において、前記復号後のコンテンツ鍵関連情報を記憶する場合に、前記記憶手段のメモリ容量を越えた場合に、当該復号後のコンテンツ鍵関連情報が記憶された時間、送信側または受信側により設定された設定情報に基づいて、当該復号後のコンテンツ鍵関連情報を削除するコンテンツ鍵関連情報削除手段を備えることを特徴とする。

【0048】かかる構成によれば、記憶手段のメモリ容量を越えた場合に、コンテンツ鍵関連情報削除手段によって、コンテンツ鍵関連情報が記憶された時間、送信側または受信側により設定された設定情報に基づいて、コンテンツ鍵関連情報が削除される。

【0049】また、請求項19記載のコンテンツ受信装置は、請求項12から請求項18のいずれか1項に記載のコンテンツ受信装置において、前記セキュリティモジュールに記憶した前記復号後のコンテンツ鍵関連情報を、前記マスター鍵で暗号化し、再暗号化コンテンツ鍵関連情報として出力し、かつ記憶するコンテンツ鍵関連情報再暗号化記憶手段を備えることを特徴とする。

【0050】かかる構成によれば、コンテンツ鍵関連情報再暗号化記憶手段によって、セキュリティモジュールに記憶されている復号後のコンテンツ鍵関連情報がマスター鍵により、再暗号化され出力され、記憶される。

【0051】また、請求項2記載のコンテンツ受信装置は、請求項19に記載のコンテンツ受信装置において、前記再暗号化コンテンツ鍵関連情報およびコンテンツを識別するコンテンツ識別子が前記記憶手段に記憶され、当該記憶手段のメモリ容量を越えた場合に、当該再暗号化コンテンツ鍵関連情報が記憶された時間、送信側または受信側により設定された設定情報に基づいて、当該再暗号化コンテンツ鍵関連情報削除手段を備えることを特徴とする。

【0052】かかる構成によれば、記憶手段のメモリ容量を越えた場合に、再暗号化コンテンツ鍵関連情報削除手段によって、再暗号化コンテンツ鍵関連情報が記憶された時間、送信側または受信側により設定された設定情報に基づいて、再暗号化コンテンツ鍵関連情報が削除される。

【0053】また、請求項21記載のコンテンツ受信装置は、請求項12から請求項16のいずれか1項に記載のコンテンツ受信装置において、前記セキュリティモジュールに記憶した前記復号後のコンテンツ鍵関連情報を、前記固有鍵で暗号化し、固有暗号化コンテンツ鍵関連情報として出力し、かつ記憶するコンテンツ鍵関連情報固有暗号化記憶手段を備えることを特徴とする。

【0054】かかる構成によれば、コンテンツ鍵関連情報固有暗号化記憶手段によって、セキュリティモジュールに記憶されている復号後のコンテンツ鍵関連情報が固有鍵により、再暗号化されて、固有暗号化コンテンツ鍵関連情報として出力され、記憶される。

【0055】また、請求項22記載のコンテンツ受信装置は、請求項21に記載のコンテンツ受信装置において、前記固有暗号化コンテンツ鍵関連情報およびコンテンツを識別するコンテンツ識別子が前記記憶手段に記憶され、当該記憶手段のメモリ容量を越えた場合に、当該固有暗号化コンテンツ鍵関連情報が記憶された時間、送信側または受信側により設定された設定情報に基づいて、当該固有暗号化コンテンツ鍵関連情報削除手段を備えることを特徴とする。

【0056】かかる構成によれば、記憶手段のメモリ容量を越えた場合に、固有暗号化コンテンツ鍵関連情報削除手段によって、固有暗号化コンテンツ鍵関連情報が記憶された時間、送信側または受信側により設定された設定情報に基づいて、固有暗号化コンテンツ鍵関連情報が削除される。

【0057】また、請求項23記載のコンテンツ受信装置は、請求項9から請求項15のいずれか1項に記載の

コンテンツ受信装置において、前記復号後のコンテンツ鍵関連情報を、前記マスター鍵で再暗号化した再暗号化コンテンツ鍵関連情報とし、この再暗号化コンテンツ鍵関連情報に対応する暗号化コンテンツと共に、記憶媒体に記憶する記憶媒体取扱手段を備えることを特徴とする。

【0058】かかる構成によれば、セキュリティモジュールに記憶された復号後のコンテンツ鍵関連情報が、記憶媒体取扱手段によって、マスター鍵により暗号化され再暗号化コンテンツ鍵関連情報とされ、暗号化コンテンツと共に、記憶媒体に記憶される。

【0059】また、請求項24記載のコンテンツ受信装置は、請求項13から請求項15のいずれか1項に記載のコンテンツ受信装置において、前記復号後のコンテンツ鍵関連情報を、前記固有鍵で再暗号化した固有暗号化コンテンツ鍵関連情報として、この固有暗号化コンテンツ鍵関連情報に対応する暗号化コンテンツと共に、記憶媒体に記憶する記憶媒体取扱手段を備えることを特徴とする。

【0060】かかる構成によれば、セキュリティモジュールに記憶された復号後のコンテンツ鍵関連情報が、記憶媒体取扱手段によって、固有鍵により暗号化され固有暗号化コンテンツ鍵関連情報とされ、暗号化コンテンツと共に、記憶媒体に記憶される。

【0061】また、請求項25記載のコンテンツ受信装置は、請求項12から請求項16および請求項19、請求項20、請求項23のいずれか1項に記載のコンテンツ受信装置において、記憶手段および記憶媒体取扱手段を備え、この記憶媒体取扱手段によって取り扱われる記憶媒体に、前記スクランブル鍵で暗号化された暗号化コンテンツと、この暗号化コンテンツを識別するコンテンツ識別子を含む前記コンテンツに関する暗号化関連情報とを記憶させるための暗号化コンテンツ関連情報記憶手段と、前記記憶媒体に記憶された前記暗号化コンテンツを再生する際に、当該暗号化コンテンツに対応する再暗号化コンテンツ鍵関連情報が前記記憶手段、前記記憶媒体の少なくとも一方に記憶されている場合、当該再暗号化コンテンツ関連情報を前記記憶手段または前記記憶媒体から読み出して、前記セキュリティモジュールに入力すると共に、前記暗号化関連情報を入力する関連情報入手手段と、前記マスター鍵により、前記再暗号化コンテンツ鍵関連情報を復号し、コンテンツ鍵を得、このコンテンツ鍵により、前記暗号化関連情報を復号し、スクランブル鍵を得、このスクランブル鍵を出力するスクランブル出力手段と、このスクランブル出力手段で出力されたスクランブル鍵で、前記記憶媒体の暗号化コンテンツを復号する暗号化コンテンツ復号手段と、を備えることを特徴とする。

【0062】かかる構成によれば、暗号化コンテンツ鍵関連情報記憶手段によって、記憶媒体に暗号化コンテンツ

とこの暗号化コンテンツに対応する暗号化関連情報とが記憶され、関連情報入力手段によって、記憶手段または記憶媒体に記憶されている再暗号化コンテンツ鍵関連情報を、セキュリティモジュールに入力し、スクランブル鍵出力手段によって、再暗号化コンテンツ鍵関連情報が復号され、コンテンツ鍵が得られ、このコンテンツ鍵により、暗号化関連情報が復号され、スクランブル鍵が得られ、暗号化コンテンツ復号手段によって、暗号化コンテンツが復号される。

【0063】また、請求項2記載のコンテンツ受信装置は、請求項13から請求項16および請求項21、請求項22、請求項24のいずれか1項に記載のコンテンツ受信装置において、記憶手段および記憶媒体取扱手段を備え、この記憶媒体取扱手段によって取り扱われる記憶媒体に、前記スクランブル鍵で暗号化された暗号化コンテンツと、この暗号化コンテンツを識別するコンテンツ識別子を含む前記コンテンツに関する暗号化関連情報とを記憶させるための暗号化コンテンツ記憶手段と、前記記憶媒体に記憶された前記暗号化コンテンツを再生する際に、当該暗号化コンテンツに対応する固有暗号化コンテンツ鍵関連情報を前記記憶手段、前記記憶媒体の少なくとも一方に記憶されている場合、当該固有暗号化コンテンツ鍵関連情報を前記記憶手段または前記記憶媒体から読み出して、前記セキュリティモジュールに入力すると共に、前記暗号化関連情報を入力する関連情報入力手段と、前記固有鍵により、前記固有暗号化コンテンツ鍵関連情報を復号し、コンテンツ鍵を得、このコンテンツ鍵により、前記暗号化関連情報を復号し、スクランブル鍵を得、このスクランブル鍵を出力するスクランブル鍵出力手段と、このスクランブル鍵出力手段で出力されたスクランブル鍵で、前記記憶媒体の暗号化コンテンツを復号する暗号化コンテンツ復号手段と、を備えることを特徴とする。

【0064】かかる構成によれば、暗号化コンテンツ関連情報記憶手段によって、記憶媒体に暗号化コンテンツとこの暗号化コンテンツに対応する暗号化関連情報とが記憶され、関連情報入力手段によって、記憶手段または記憶媒体に記憶されている固有暗号化コンテンツ鍵関連情報を、セキュリティモジュールに入力し、スクランブル鍵出力手段によって、固有暗号化コンテンツ鍵関連情報が復号され、コンテンツ鍵が得られ、このコンテンツ鍵により、暗号化関連情報が復号され、スクランブル鍵が得られ、暗号化コンテンツ復号手段によって、暗号化コンテンツが復号される。

【0065】また、請求項27記載のコンテンツ受信装置は、請求項9から請求項26のいずれか1項に記載のコンテンツ受信装置において、前記暗号化コンテンツを送信中に、当該暗号化コンテンツを記憶しなかった場合、当該暗号化コンテンツに対応するコンテンツ鍵を記憶しないコンテンツ鍵不記憶手段を備えることを特徴と

する。

【0066】かかる構成によれば、コンテンツ鍵不記憶手段によって、暗号化コンテンツを記憶しない場合、この暗号化コンテンツに対応するコンテンツ鍵、すなわち、暗号化コンテンツ鍵関連情報が記憶されない。

【0067】また、請求項28記載のコンテンツ受信装置は、請求項9から請求項27のいずれか1項に記載のコンテンツ受信装置において、前記暗号化関連情報を、コンテンツ鍵で復号するタイミングで、当該暗号化関連情報に対応するコンテンツの送信開始時刻、終了時刻に基づいて、当該コンテンツ鍵を切り替えるコンテンツ鍵切替手段を備えることを特徴とする。

【0068】かかる構成によれば、コンテンツ鍵切替手段によって、暗号化関連情報をコンテンツ鍵で復号するタイミングがコンテンツの送信開始時刻、終了時刻に基づいて、切り替えられる。

【0069】さらにまた、請求項29記載のコンテンツ送信プログラムは、デジタル放送におけるコンテンツを暗号化して送信するコンテンツ送信装置を、以下に示す手段として機能させることを特徴とする。コンテンツ送信装置を機能させる手段は、経過時間と共に変更されるスクランブル鍵と、前記コンテンツ毎に設けられたコンテンツ鍵と、前記コンテンツの継続時間よりも長時間にわたり保持されるワーク鍵と、受信側に共通に備えられたマスター鍵とを記憶する記憶手段、前記スクランブル鍵により、前記コンテンツを暗号化し暗号化コンテンツとするコンテンツ暗号化手段、前記コンテンツ鍵により、少なくとも前記スクランブル鍵を含む前記コンテンツに関する関連情報を暗号化し暗号化コンテンツとする関連情報暗号化手段と、前記ワーク鍵により、少なくとも前記コンテンツ鍵を含む当該ワーク鍵に関する関連情報を暗号化し暗号化ワーク鍵関連情報とするワーク鍵関連情報暗号化手段、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報を多重化し多重暗号化コンテンツとする多重化手段、この多重化手段で多重化された多重暗号化コンテンツを送信する多重暗号化コンテンツ送信手段、である。

【0070】かかる構成によれば、まず、送信されるコンテンツが経過時間と共に変更されるスクランブル鍵によって暗号化され、暗号化コンテンツとされる。そして、スクランブル鍵もコンテンツ毎に設けられたコンテンツ鍵によって、コンテンツに関する関連情報と共に、暗号化され、暗号化関連情報とされる。また、コンテンツ鍵もコンテンツの継続時間よりも長時間にわたり保持されるワーク鍵によって、コンテンツ鍵に関する関連情報と共に、暗号化され、暗号化コンテンツ鍵関連情報と

される。さらに、ワーク鍵も受信側に共通に備えられたマスター鍵によって、ワーク鍵に関する関連情報と共に、暗号化され、暗号化ワーク鍵関連情報とされる。その後、暗号化されたこれらの情報が多重化され、送信される。

【0071】そしてまた、請求項30記載のコンテンツ受信プログラムは、送信側でデジタル放送におけるコンテンツが暗号化され、この暗号化されたコンテンツを受信するコンテンツ受信装置を、以下に示す手段として機能させることを特徴とする。コンテンツ受信装置を機能させる手段は、前記送信側に共通に備えられたマスター鍵を記憶する記憶手段、前記送信側において、経過時間と共に変更されるスクランブル鍵により前記コンテンツが暗号化された暗号化コンテンツと、前記コンテンツ毎に設けられたコンテンツ鍵により、少なくとも前記スクランブル鍵を含む前記コンテンツに関する関連情報が暗号化された暗号化関連情報と、前記コンテンツの継続時間よりも長時間にわたり保持されるワーク鍵により、少なくとも前記コンテンツ鍵を含む当該コンテンツに関する関連情報が暗号化された暗号化コンテンツ鍵関連情報と、前記マスター鍵により、少なくとも前記ワーク鍵を含む当該ワーク鍵に関する関連情報が暗号化された暗号化ワーク鍵関連情報とが多重化された多重暗号コンテンツが送信され、この多重暗号コンテンツを受信する多重暗号コンテンツ受信手段、この多重暗号コンテンツ受信手段で受信した多重暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記ワーク鍵関連情報に分離する多重暗号コンテンツ分離手段、当該暗号化ワーク鍵関連情報を前記マスター鍵で復号し、復号されたワーク鍵で前記暗号化コンテンツ鍵関連情報に含まれるコンテンツ鍵を復号し、復号されたコンテンツ鍵で前記暗号化関連情報に含まれるスクランブル鍵を復号し、復号されたスクランブル鍵で前記暗号化コンテンツを復号し前記コンテンツを得る多重暗号コンテンツ復号手段、である。

【0072】かかる構成によれば、まず、送信側で多重化された多重暗号コンテンツが、多重暗号コンテンツ受信手段によって、受信される。そして、受信された多重暗号コンテンツは、多重暗号コンテンツ分離手段によって、暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報に分離される。その後、多重暗号コンテンツ復号手段によって、マスター鍵により暗号化ワーク鍵関連情報が復号され、ワーク鍵が得られ、このワーク鍵により暗号化コンテンツ鍵関連情報が復号され、コンテンツ鍵が得られ、このコンテンツにより暗号化関連情報が復号され、スクランブル鍵が得られ、このスクランブル鍵により暗号化コンテンツが復号され、コンテンツが得られる。

【0073】

【発明の実施の形態】以下、本発明の一実施形態を図面

に基づいて詳細に説明する。

（限定受信システムの構成、コンテンツ鍵とコンテンツとを併せて送信する場合）図1は、限定受信システムの全体構成を图示したものである。この図1に示すように、限定受信システム1は、コンテンツ送信装置3とコンテンツ受信装置5とから構成され、コンテンツ送信装置3は、コンテンツスクランブル部7と、多重化部9と、記憶部11とを備えて構成されている。コンテンツ受信装置5は、分離部13と、コンテンツデスクランブル部15と、記憶部17とを備えて構成されている。

【0074】限定受信システム1は、デジタル放送において、暗号化したコンテンツ（放送番組）を送信し、受信側で暗号化されたコンテンツを復号し、視聴するシステムであって、暗号化したコンテンツを復号するのに、特別の限定された受信装置を要するもの（ゆえに、限定受信システムと称呼される）である。

【0075】コンテンツ送信装置3は、コンテンツを暗号化して受信側のコンテンツ受信装置5に送信するものであって、映像・音声データあるコンテンツを、受信側と共通に備えられるマスター鍵を利用して（ゆえに、共通鍵暗号化方式と称呼される）暗号化し、送信するものである。

【0076】コンテンツスクランブル部7は、まず、図示を省略した暗号キー生成装置（後記する）で生成されたスクランブル鍵Ksを用いて、送信するコンテンツを暗号化し暗号化コンテンツとする（暗号化器7a）。次に、記憶部11に記憶されているコンテンツ鍵Kcを用いて、少なくともスクランブル鍵を含んだコンテンツに関する関連情報を暗号化し暗号化関連情報とする（暗号化器7b）。また、記憶部11に記憶されているワーク鍵Kwを用いて、少なくともコンテンツ鍵を含んだ当該コンテンツに関する関連情報を暗号化し暗号化コンテンツ鍵関連情報とする（暗号化器7c）。さらに、記憶部11に記憶されているマスター鍵Km0を用いて、少なくともワーク鍵を含んだワーク鍵に関する関連情報を暗号化し暗号化ワーク鍵関連情報とする（暗号化器7d）。

【0077】ここで、コンテンツ送信装置3のコンテンツスクランブル部7と請求項に記載した要件との対応関係を補足すると、暗号化器7aがコンテンツ暗号化手段に、暗号化器7bが関連情報暗号化手段に、暗号化器7cがコンテンツ鍵関連情報暗号化手段に、暗号化器7dがワーク鍵関連情報暗号化手段に対応（相当）している。

【0078】多重化部9は、コンテンツスクランブル部7で暗号化した、暗号化コンテンツと、暗号化関連情報と、暗号化コンテンツ鍵関連情報と、暗号化ワーク鍵関連情報とを多重化し、多重暗号コンテンツを生成し、受信側に送出するものである。この多重化部9が請求項に記載した多重化手段と多重暗号コンテンツ送信手段とに

相当するものである。

【0079】記憶部11は、経過時間と共に変更されるスクランブル鍵Ks、コンテンツ毎に備えられているコンテンツ鍵Kc、コンテンツの継続時間よりも長時間にわたり保持されるワーク鍵Kw、コンテンツ受信装置5に備えられる送受信間で共通のマスター鍵Kmを記憶するものである。

【0080】なお、この図1において、図示を省略したが、記憶部11に記憶されている各暗号キーを生成する暗号キー生成装置が備えられている。また、このコンテンツ送信装置3には、図示を省略した暗号化コンテンツ鍵関連情報送信手段と、コンテンツ鍵関連情報記憶指定手段と、コンテンツ鍵関連情報利用指定手段と、固有鍵設定用関連情報暗号化手段とを備えている。

【0081】暗号化コンテンツ鍵関連情報送信手段は、暗号化コンテンツ鍵関連情報と、多重暗号コンテンツの送信開始時刻後の所定の時間、または、多重暗号コンテンツの送信を開始する送信開始時刻より所定の時間前から送信終了時刻の所定の時間後まで、所定の時間間隔で繰り返し送信する、或いは、受信側で暗号化コンテンツ鍵関連情報を受信していない場合に、受信側からの要求に基づいて送信する若しくは通信回線網を介して送信するか、の少なくとも一つの手段により、暗号化コンテンツ鍵関連情報を送信するものである。

【0082】コンテンツ鍵関連情報記憶指定手段は、コンテンツ受信装置5で暗号化コンテンツ鍵関連情報を復号しコンテンツ鍵関連情報とした後、当該コンテンツ鍵関連情報を、そのまま、或いは別途暗号化して保持する際に、受信側のコンテンツ受信装置5が後記する記憶手段、記憶媒体を取り扱う記憶媒体取扱手段の少なくとも一方を備える場合、後記するセキュリティモジュール、記憶手段、記憶媒体のいずれかに保持させることを指定するものである。

【0083】コンテンツ鍵関連情報利用指定手段は、受信側で記憶媒体を取り扱う記憶媒体取扱手段を備える際に、当該記憶媒体に暗号化コンテンツが記憶され、当該暗号化コンテンツが再生されるときに、当該暗号化コンテンツに対応する暗号化コンテンツ鍵関連情報を送信している場合には、当該暗号化コンテンツ鍵関連情報を利用せずに、保持されたコンテンツ鍵関連情報を利用するように指定するものである。

【0084】固有鍵設定用関連情報暗号化手段は、コンテンツ受信装置5に備えられるセキュリティモジュール毎に、当該セキュリティモジュールに入力される情報を暗号化する、複数の固有鍵（後記するグループ鍵Kgに相当する）が当該セキュリティモジュール内部に設定されており、これら固有鍵を、マスター鍵Kmで暗号化し暗号化固有鍵設定用関連情報とするものである。

【0085】また、一方、コンテンツ受信装置5は、送信側のコンテンツ送信装置2で暗号化され、多重化され

た多重暗号コンテンツを受信し、この多重暗号コンテンツを復号し、視聴可能にするものである。分離部13は、送信側のコンテンツ送信装置3から送信された多重暗号コンテンツを受信すると共に、この多重暗号コンテンツを、暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報に分離するものである。この分離部13が請求項に記載した多重暗号コンテンツ受信手段と多重暗号コンテンツ分離手段とに相当するものである。

【0086】コンテンツデスクランブル部15は、4つの復号器（後記するセキュリティモジュールSM）を備えて構成されており、分離部13で分離された暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報を復号するものであって、まず、暗号化ワーク鍵関連情報がマスター鍵により復号されワーク鍵が得られ（復号器15a）、このワーク鍵により暗号化コンテンツ鍵関連情報が復号されコンテンツ鍵が得られ（復号器15b）、このコンテンツ鍵により暗号化関連情報が復号されスクランブル鍵が得られ（復号器15c）、このスクランブル鍵により暗号化コンテンツが復号され、コンテンツが得られる（復号器15d）。このコンテンツデスクランブル部15が、請求項に記載した多重暗号コンテンツ復号手段に相当するものである。

【0087】記憶部17は、コンテンツ受信装置5本体に一体的に備えられているメモリ部17a（触覚項目に記載した記憶手段に相当する）と、記憶媒体に情報を記憶させる記憶媒体取扱手段17bとを備えて構成されている。また、コンテンツ受信装置5には、この図1において図示を省略したセキュリティモジュールSMが備えられている。このセキュリティモジュールSMは、少なくとも復号器15a～15cを備え、マスター鍵Kmが保持されるものであって、外部より読み出し不可能なICカード等から構成されている。

【0088】また、コンテンツ受信装置5は、図示を省略した暗号化コンテンツ鍵関連情報要求手段と、コンテンツ鍵関連情報記憶手段と、暗号化固有鍵設定用関連情報受信手段と、暗号化固有鍵設定用関連情報復号手段と、コンテンツ鍵関連情報出力手段と、コンテンツ鍵関連情報再暗号化記憶手段と、コンテンツ鍵関連情報固有暗号化記憶手段と、コンテンツ鍵不記憶手段と、コンテンツ鍵切替手段とを備えている。なお、これらは、図示を省略したコンテンツ受信装置5の主制御部に展開しているプログラムである。

【0089】暗号化コンテンツ鍵関連情報要求手段は、コンテンツ受信装置5において、暗号化コンテンツ鍵関連情報が得られていない場合に、送信側のコンテンツ送信装置3に暗号化コンテンツ鍵関連情報を要求するものである。コンテンツ鍵関連情報記憶手段は、復号後のコンテンツ鍵関連情報およびこのコンテンツに鍵関連情報

に係り、コンテンツを識別するコンテンツ識別子をセキュリティモジュールSMに記憶させるものである。

【0090】暗号化固有鍵設定用関連情報受信手段は、セキュリティモジュールSMに固有鍵が複数設けられており、送信側のコンテンツ送信装置3において、マスター鍵Kmにより、これらの固有鍵が暗号化され、暗号化固有鍵設定用関連情報とされ、この暗号化固有鍵設定用関連情報を受信するものである。暗号化固有鍵設定用関連情報復号手段は、暗号化固有鍵設定用関連情報受信手段で受信した暗号化固有鍵設定用関連情報をマスター鍵Kmにより復号するものである。

【0091】コンテンツ鍵関連情報出力手段は、セキュリティモジュールSMに記憶した復号後のコンテンツ鍵関連情報を出力し、記憶部17に記憶させるものである。コンテンツ鍵関連情報再暗号化記憶手段は、セキュリティモジュールSMに記憶した復号後のコンテンツ鍵関連情報を、セキュリティモジュールSM内に設定されているマスター鍵Kmで暗号化し、再暗号化コンテンツ鍵関連情報として出力し、記憶部17に記憶させるものである。

【0092】コンテンツ鍵関連情報固有暗号化記憶手段は、セキュリティモジュールSMに記憶した復号後のコンテンツ鍵関連情報を、セキュリティモジュールSM内に設定されている固有鍵（後記するグループ鍵Kgに相当する）で暗号化し、固有暗号化コンテンツ鍵関連情報として出力し、記憶部17に記憶させるものである。コンテンツ鍵不記憶手段は、暗号化コンテンツを送信中に、当該暗号化コンテンツを記憶部17に記憶しなかった場合、当該暗号化コンテンツに対応するコンテンツ鍵（暗号化コンテンツ鍵関連情報）を記憶しないものである。

【0093】コンテンツ鍵切替手段は、暗号化関連情報を、コンテンツ鍵で復号するタイミングを、当該暗号化関連情報に対応するコンテンツの送信開始時刻、終了時刻に基づいて、当該コンテンツ鍵を切り替えるものである。

【0094】ここで、コンテンツの暗号化、復号の流れに沿って説明する。コンテンツは、コンテンツ送信装置3のコンテンツスクランブル部7において、共通暗号化方式を用いてスクランブル化され、スクランブル鍵Ks、コンテンツ鍵Kc、ワーク鍵Kwのそれぞれを含む暗号化された関連情報と多重化され送出される。送出されたコンテンツは、コンテンツ受信装置5のコンテンツ分離部13において、各々の鍵を含む関連情報とスクランブル化されたコンテンツとに分離され、スクランブル化されたコンテンツをコンテンツデスクランブル部15でデスクランブル化し、平文（復号後のコンテンツ）が得られる。

【0095】また、コンテンツ受信装置5において、コンテンツは、記憶部17に記憶され、利用時（コンテン

ツ再生時）に、コンテンツデスクランブル部15でデスクランブル化され、利用される。なお、マスター鍵Kmは、コンテンツ受信装置5またはセキュリティモジュールSMに割り当てられた特有の鍵であって、このマスター鍵Kmは予め、コンテンツ受信装置5またはセキュリティモジュールSM内に書き込まれている。

【0096】またここで、複数のコンテンツ受信装置5に対して、ワーク鍵Kwを共有させる場合について説明する。まず、送信側のコンテンツ送信装置3は、該当するコンテンツ受信装置5のマスター鍵Kmを記憶部11に保持されているマスター鍵データベース（図示せず）より読み出す。そして、この読み出したマスター鍵Kmによりワーク鍵Kwを共通暗号方式により暗号化する。さらに、暗号化されたワーク鍵を含む関連情報と、例えば、MPEG-2多重化方式のセクション形式でパケット化し個別情報として、多重化部9でコンテンツと併せてトランスポートストリームとして多重化する。

【0097】なお、このパケット化の例として、ARIBの限定受信方式規格（STD-B25）に記載された

20 EMM（Entitlement Management Message）形式が利用できる。コンテンツ受信装置5では、分離部13において、受信したMPEG-2トランスポートストリームからEMMを取り出し、マスター鍵Kmを用いて復号し、ワーク鍵Kwを得る。そして、この動作を、各コンテンツ受信装置5に対して繰り返し実行し、複数のコンテンツ受信装置5においてワーク鍵Kwが共有される。

【0098】コンテンツ受信装置5において、得られたワーク鍵Kwは、セキュリティモジュールに記憶され、保持される。なお、複数のコンテンツ受信装置5間で共有化されたワーク鍵Kwは、ワーク鍵Kw自体の安全性を確保するために、例えば、1ヶ月や1年といった期間で更新される。また、このワーク鍵Kwはコンテンツとは独立に放送帯域の空の帯域を利用して順次送信することも可能である。また、場合によっては、予め、セキュリティモジュールSMにワーク鍵Kwを書き込んで配布することも可能である。

【0099】さらにここで、スクランブル鍵およびコンテンツ鍵について補足説明をする。スクランブル鍵Ksは、コンテンツをスクランブル化する鍵であって、不正受信に対する安全性を高めるために、1秒程度の時間で変更されるように設定されたものである。スクランブル鍵Ksは、コンテンツ鍵Kcにより共通暗号方式によって暗号化される。暗号化されたスクランブル鍵Ksは、MPEG-2多重化方式のセクション形式でパケット化され共通情報として多重化部9でコンテンツと併せてトランスポートストリームとして多重化する。

【0100】このパケット化の具体的な方式の例として、ARIBの限定受信方式規格（STD-B25）に記載されたECM（Entitlement Cont

rolMessage)形式で利用できる。なお、スクランブル鍵Ksの送出時間については後記する。

【0101】コンテンツ鍵Kcは、コンテンツ各々に割り当てられたコンテンツ固有の鍵であり、このコンテンツ鍵Kcは、ワーク鍵Kwにより共通暗号方式によって暗号化される。暗号化されたコンテンツ鍵Kcは、MPEG-2多重化方式のセクション形式でパケット化され共通情報(暗号化コンテンツ鍵関連情報)として多重化部9でコンテンツと併せてトランスポートストリームとして多重化される。

【0102】さらにここで、限定受信システム1を利用して、放送されているコンテンツをリアルタイムに視聴する場合について補足説明する。コンテンツをリアルタイムに視聴する場合、例えば、送信側のコンテンツ送信装置3からコンテンツ(多重暗号コンテンツ)を送出する所定時間前からコンテンツ鍵(暗号化コンテンツ鍵関連情報)の送出を開始し、コンテンツを送出している間、コンテンツ鍵を所定時間間隔で繰り返し送出させ、コンテンツの送出終了後(放送終了後)、コンテンツ鍵の送出も終了させる。一方、受信側のコンテンツ受信装置5において、記憶部17に送信されたコンテンツを記憶後、記憶しておいたコンテンツを再生して視聴する場合には、視聴するまではコンテンツ受信装置5の記憶部17にスクランブル化されたまま、コンテンツを記憶しておき、コンテンツを視聴するときに、コンテンツ鍵を送出する方法がとられる。

【0103】次に、図2を参照して、スクランブル鍵Ks、コンテンツ鍵Kc、ワーク鍵Kwをパケット化する際のファイルフォーマットについて説明する。関連情報S(共通情報S)は、スクランブル鍵の送出に用いられる番組情報であり、事業者ID、コンテンツID、スクランブル鍵Ks等から構成されている。事業者IDは放送事業者に割り当てられた識別子であり、コンテンツIDは、コンテンツ毎にユニークに、或いは、所定の条件(例えば、再放送番組を同一IDとするか別のIDとするか等の条件)に基づいて、割り当てられた識別子である。そして、スクランブル鍵Ksは、コンテンツIDに対応するコンテンツ鍵Kcによって暗号化されている。

【0104】コンテンツ鍵関連情報C(共通情報C)は、コンテンツ鍵Kcの送出に用いられる共通の情報であり、事業者ID、ワーク鍵ID、コンテンツID、コンテンツ鍵等から構成されている。事業者IDは放送事業者に割り当てられた識別子であり、ワーク鍵IDはワーク鍵を識別する識別子であり、コンテンツIDは、コンテンツ毎にユニークに、割り当てられた識別子である。これらのうち少なくともコンテンツ鍵は、ワーク鍵IDに対応するワーク鍵によって暗号化されている。

【0105】ワーク鍵関連情報W(個別情報W)は、ワーク鍵Kwの送出に用いられる個別情報であり、事業者ID、カードID、更新番号、有効期限、ワーク鍵ID

D、ワーク鍵等から構成されている。事業者IDは、放送事業者或いはその特定の集合(グループ)等に割り当てられた識別子であり、カードIDは、セキュリティモジュールSM毎に割り当てられた識別子であり、更新番号は、ワーク鍵Kwのバージョンを示す番号であり、有効期限は、ワーク鍵Kwの有効期限を示すものである。そして、ワーク鍵Kwは、カードIDに対応するマスター鍵Kmによって暗号化されている。

【0106】(コンテンツ受信装置とセキュリティモジュールとの関係(構成))次に、図3を参照して、限定受信システム1におけるコンテンツ受信装置5とセキュリティモジュールSM1との関係を説明する。コンテンツ受信装置5は、受信したストリーム(多重暗号コンテンツ)からワーク鍵Kwとコンテンツ鍵Kcを含む関連情報を分離するKw・Kc関連情報分離部13aと、暗号化コンテンツを記憶する記憶部17aと、スクランブル鍵Ksを含む関連情報を分離するKs関連情報分離部13bと、コンテンツをデスクランブルするコンテンツデスクランブル部15と、コンテンツ受信装置5とセキュリティモジュールSM1との通信を行うインターフェース(図示せず)等から構成されている。

【0107】セキュリティモジュールSM1は、マスター鍵Kmを備え、4つの復号器(19a~19d)と、1つの暗号化器21と、状況に応じて入力される複数の情報を制御するソフトウェアスイッチS/Wとを備えて構成されている。このソフトウェアスイッチS/Wに、入力される情報数は3個であり、この情報数に対応してa1~a3のスイッチが備えられており、スイッチa1がリアルタイムにコンテンツを視聴する場合、スイッチa2が記憶再生視聴する場合、スイッチa3が取寄せ放送の視聴の場合に対応している。

【0108】Kw・Kc関連情報分離部13aで、多重暗号コンテンツから暗号化ワーク鍵関連情報を抽出し、この暗号化ワーク鍵関連情報に記述されているカードIDと、セキュリティモジュールSM1(この実施の形態ではICカード)のカードIDとが一致する場合、ワーク鍵Kw、ワーク鍵ID、更新番号、有効期限、事業者IDとが含まれている暗号化ワーク鍵関連情報をセキュリティモジュールSM1に入力する。セキュリティモジュールSM1では、入力された暗号化されているワーク鍵Kwをマスター鍵Kmで復号し、ワーク鍵Kwを得て(復号器19a)、このワーク鍵Kwは、事業者ID、更新番号、有効期限、ワーク鍵IDとに対応させて、セキュリティモジュールSM1内で保持される。

【0109】一方、Kw・Kc関連情報分離部13aにおいて、暗号化コンテンツ鍵関連情報を抽出し、ワーク鍵IDと、暗号化されているコンテンツ鍵Kc、事業者ID、有効期限、コンテンツIDとが含まれている暗号化コンテンツ鍵関連情報をセキュリティモジュールSM1に入力する。セキュリティモジュールSM1では、暗

号化コンテンツ鍵関連情報をワーク鍵IDに対応するワーク鍵Kwを用いて復号し、コンテンツ鍵Kcを得る(復号器19b)。

【0110】(暗号化コンテンツの再生例(リアルタイム視聴))次に、図3に図示したコンテンツ受信装置5およびセキュリティモジュールSM1を用いて、送信されているコンテンツ(リアルタイム)を視聴する場合について説明する。リアルタイムにコンテンツを視聴する場合であるので、予め、セキュリティモジュールSM1のソフトウェアスイッチS/Wをa1に切り替えておく。

【0111】Kw・Kc関連情報分離部13aの出力は、Ks関連情報分離部13bに入力される。Ks関連情報分離部13bでは、関連情報Sを抽出し、コンテンツIDと暗号化されたスクランブル鍵Ksを含む関連情報SをセキュリティモジュールSM1に入力する。セキュリティモジュールSM1では、関連情報SをコンテンツIDに対応するコンテンツ鍵Kcを用いて復号し、スクランブル鍵Ksを得る(復号器19d)。そして、得られたスクランブル鍵Ksがコンテンツ受信装置5に出力され、コンテンツ受信装置5では、入力されたスクランブル鍵Ksを用いて、コンテンツデスクランブル部15で暗号化コンテンツを復号し、コンテンツを出力する。

【0112】(暗号化コンテンツの再生例(記憶再生視聴))次に、図3に図示したコンテンツ受信装置5およびセキュリティモジュールSM1を用いて、記憶部17aに記憶したコンテンツを視聴する場合について説明する。記憶部17aに記憶させたコンテンツを視聴する場合であるので、予め、セキュリティモジュールSM1のソフトウェアスイッチS/Wをa2に切り替えておく。

【0113】暗号化コンテンツはそのまま(スクランブル化されたまま)、暗号化されたスクランブル鍵を含む暗号化関連情報(関連情報S)と共に、コンテンツIDと対応されて、記憶部17aに記憶されている。一方、Kw・Kc関連情報分離部13aにおいて、暗号化コンテンツ鍵関連情報(コンテンツ鍵関連情報C)を抽出し、抽出した、暗号化されたコンテンツ鍵を含む暗号化コンテンツ鍵関連情報をセキュリティモジュールSM1に入力する。そして、復号器19bで復号されたコンテンツ鍵を、マスター鍵を用いて暗号化する(暗号化部21)。この暗号化されたコンテンツ鍵Kcをコンテンツ受信装置5に出力し、記憶部17aに記憶されている暗号化コンテンツと対応させて記憶する。

【0114】そして、記憶部17aに記憶されているコンテンツを再生するときには、デスクランブルするコンテンツに対応する、暗号化されたコンテンツ鍵を記憶部17aから読み出して、セキュリティモジュールSM1に入力する。セキュリティモジュールSM1では、入力された、暗号化されているコンテンツ鍵をマスター鍵K

mにより、復号しコンテンツ鍵Kcを得る(復号器19c)。また一方、再生されたコンテンツは、Ks関連情報分離部13bに入力され、暗号化関連情報(関連情報S)を抽出し、抽出した、暗号化されているスクランブル鍵Ksを含む暗号化関連情報(関連情報S)をセキュリティモジュールSM1に入力する。

【0115】セキュリティモジュールSM1では、入力された、暗号化されているスクランブル鍵を復号器19cで復号されたコンテンツ鍵で復号し、スクランブル鍵Ksを得る(復号器19d)。このスクランブル鍵Ksをコンテンツ受信装置5に出力する。コンテンツ受信装置5のコンテンツデスクランブル部15(15d)に入力されたスクランブル鍵により、暗号化コンテンツが復号され、コンテンツが出力される。

【0116】また、コンテンツ受信装置5にホームネットワーク等を介して、記憶装置(図示せず)が接続されている場合には、Ks関連情報分離部13bに入力される前に、ストリーム(多重暗号コンテンツの一部)が、ホームネットワーク等を介して、コンテンツ受信装置5以外の記憶装置に記憶される。このとき、暗号化コンテンツおよび暗号化関連情報と併せて、マスター鍵Kmで暗号化した再暗号化コンテンツ鍵を記憶装置に記憶させる。暗号化コンテンツの再生時には、記憶装置で再生された信号(スクランブルされたままのコンテンツ信号)がコンテンツ受信装置5のKs関連情報分離部13bにホームネットワークを介して入力されると共に、コンテンツ受信装置5を介して再暗号化コンテンツ鍵がセキュリティモジュールSM1に入力され、復号器19cで再暗号化コンテンツ鍵が復号され、復号器19dでスクランブル鍵Ksが得られ、コンテンツがデスクランブルされる。

【0117】(既存のBSデジタル放送(暗号化コンテンツ)の再生例(リアルタイム視聴))次に、図3に図示したコンテンツ受信装置5およびセキュリティモジュールSM1を用いて、既存のBSデジタル放送(暗号化コンテンツ)を、リアルタイムで視聴する場合について説明する。既存のBSデジタル放送(暗号化コンテンツ)を視聴する場合であるので、予め、セキュリティモジュールSM1のソフトウェアスイッチS/Wをa3に切り替えておく。

【0118】まず、暗号化コンテンツと共に多重化される、暗号化ワーク鍵関連情報を図6に示すファイルフォーマットを参照して説明する。図6に示すように、暗号化ワーク鍵関連情報ECM-Kwは、事業者ID、ワーク鍵ID、スクランブル鍵ID等から構成されている。スクランブル鍵Ksはワーク鍵IDに対応するワーク鍵IDによって暗号化されている。

【0119】このとき、復号器19aと、復号器19dと、コンテンツデスクランブル部15dとをBSデジタル放送で使用されている暗号化方式と同一の方式とすれ

ば、暗号化されたスクランブル鍵Ksを含む関連情報(ECM-Kw)を復号器19dに入力し、復号器19aで得られたワーク鍵Kwを用いて復号し、得られたスクランブル鍵Ksをコンテンツ受信装置5に出力すれば、コンテンツ受信装置5では、BSデジタル放送の暗号化コンテンツをデスクランブルすることが可能である。

【0120】(既存のBSデジタル放送(暗号化コンテンツ)の再生例(記憶再生視聴))次に、図9に図示したコンテンツ受信装置5およびセキュリティモジュールSM1を用いて、既存のBSデジタル放送(暗号化コンテンツ)を記憶後、視聴する場合について説明する。既存のBSデジタル放送(暗号化コンテンツ)を視聴する場合であるので、予め、セキュリティモジュールSM1のソフトウェアスイッチS/Wをa3に切り替えておく。

【0121】(ローカル暗号化を用いる方法)図9に、ローカル暗号化を用いる方法に供される、コンテンツ受信装置5とセキュリティモジュールSM1とを示す。既存のBSデジタル放送による受信した暗号化コンテンツは、一旦、コンテンツデスクランブル部15で復号され、ローカル暗号化部23で暗号化され、記憶部17aに記憶される。なお、ローカル暗号とは、共通鍵暗号化方式等を用いて、共通鍵を独自に生成して、コンテンツを暗号化し、この暗号化したコンテンツに共通鍵を対応させて記憶手段に記憶させることをいう。

【0122】ローカル暗号化部23で暗号化されたコンテンツを復号する場合には、ローカル復号部25で、コンテンツを暗号化した共通鍵が用いられて復号される。そして、この復号されたコンテンツをホームネットワーク経由で、コンテンツ受信装置5以外の記憶装置(図示せず)等に配信する場合には、復号されたコンテンツがDTPC(Digital Transmission Content Protection)等のコンテンツを保護する保護技術によって、暗号化後配信される。そして、配信先の記憶装置(図示せず)において、コンテンツ保存時にローカル暗号が施され、記憶される等の方法が用いられる。

【0123】(ワーク鍵Kwを用いる方法)図10に、ワーク鍵Kwを用いる方法に供される、コンテンツ受信装置5とセキュリティモジュールSM2とを示す。予め、セキュリティモジュールSM2のソフトウェアスイッチS/Wをa3に切り替えておく。

【0124】既存のBSデジタル放送により受信した暗号化コンテンツは、スクランブル化されたまま、暗号化されたスクランブル鍵が含まれる暗号化関連情報ECM-Kw(図6参照)と共に、記憶部17aに記憶される。一方、Kw・Kc関連情報分離部13aにおいて、暗号化されたワーク鍵Kwを含む暗号化ワーク鍵関連情報EMM(Kw配布用、図6参照)をセキュリティモジ

ュールSM2に入力し、復号器19aでマスター鍵Kmにより復号され、ワーク鍵Kwを得て、このワーク鍵Kw(コンテンツの放送開始時刻よりも前にセキュリティモジュールSM2に記憶されている)を暗号化装置21入力し、マスター鍵Kmを用いて暗号化する。暗号化されたワーク鍵Kwをコンテンツ受信装置5に出力する。コンテンツ受信装置5では、記憶部17aに記憶されている暗号化コンテンツと、暗号化されたワーク鍵Kwと、ワーク鍵IDとを対応させて記憶させる。

10 【0125】次に、記憶部17aに記憶されている暗号化コンテンツを再生するときには、デスクランブルする暗号化コンテンツに対応する暗号化されたワーク鍵Kwを記憶部17aから読み出して、セキュリティモジュールSM2に入力する。セキュリティモジュールSM2では、復号器19cでマスター鍵Kmを用いて、暗号化されたワーク鍵Kwを復号し、ワーク鍵Kwを得る。一方、再生された暗号化コンテンツは、Ks関連情報分離部13bで暗号化されたスクランブル鍵Ksを含む暗号化関連情報ECM-Kwを分離し、セキュリティモジュールSM2に入力する。セキュリティモジュールSM2では、ソフトウェアスイッチS/Wをa2に切り替えて、入力された暗号化関連情報ECM-Kwを復号器19dに入力し、ワーク鍵Kwで復号し、スクランブル鍵Ksを得て、このスクランブル鍵Ksをコンテンツ受信装置5に出力する。コンテンツ受信装置5では、入力されたスクランブル鍵Ksをコンテンツデスクランブル部15に入力し暗号化コンテンツをデスクランブルする。

30 【0126】(コンテンツ受信装置に入力されるストリーム(暗号化コンテンツ)に対する各鍵の時間変化の例)次に、図4を参照して、コンテンツ受信装置5に入力されるストリーム(多重暗号コンテンツ)に対する、スクランブル鍵Ks、コンテンツ鍵Kc、ワーク鍵Kwの時間変化を説明する。ここでは、コンテンツリアルタイムに視聴される場合を想定しており、コンテンツA、コンテンツB、コンテンツCが連続して放送される場合について説明する。コンテンツAが放送されている間は、コンテンツIDは000Aとして送出され、コンテンツBが放送されると、コンテンツIDは000Bに切り替えられ、コンテンツCが放送されると、コンテンツIDは000Cに切り替えられて送出される。

40 【0127】スクランブル鍵KsA1、KsA2・・・KsAnは、コンテンツAを放送中に、KsA1からKsAnまで、数秒程度の単位時間で変更され、コンテンツAをスクランブルする。このスクランブル鍵KsA1・・・KsAnは、コンテンツAの放送が開始される数秒前から配信される。つまり、任意のコンテンツのスクランブルに用いたスクランブル鍵Ksは、このスクランブル鍵Ksを用いてスクランブルした暗号化コンテンツの送信よりも先に配信される。

【0128】次に、コンテンツBに切り替わる数秒前からスクランブル鍵K s B1が送出され、コンテンツBの放送になると、K s B1からK s Bnまで、数秒程度の単位時間でスクランブル鍵K s B1〜K s Bnが変更される。同様に、スクランブル鍵K s C1、K s C2、・・・K s CnはコンテンツCを放送中に数秒程度の単位時間で変更される。

【0129】コンテンツ鍵K c Aはスクランブル鍵K s A1からK s Anまでを、コンテンツ鍵K c Bはスクランブル鍵K s B1からK s Bnまでを、コンテンツ鍵K c Cはスクランブル鍵K s C1からK s Cnまでを暗号化している鍵である。この図4に示したように、コンテンツAが放送されている間は、同じコンテンツ鍵K c Aが用いられ、コンテンツAが終了し、コンテンツBが放送されると、コンテンツ鍵K c Bに変更される。同様にコンテンツCが放送されると、コンテンツ鍵K c Cに変更される。コンテンツ鍵K c A、K c B、K c Cは、対象となるコンテンツが放送される数秒前から送出され、対象となるコンテンツが放送中であれば、数秒程度の単位時間で対応するコンテンツ鍵K cが繰り返し送出され、対象となるコンテンツの放送終了後、対応するコンテンツ鍵K cの送出も停止される。なお、ここでは敢えて、コンテンツ鍵K cと記述したが、実際には、暗号化コンテンツ鍵関連情報に含まれた形式で、暗号化コンテンツ鍵として、コンテンツ受信装置5に受信される。

【0130】次に、スクランブル化されたコンテンツが一旦記憶され、再生する場合における各鍵の取扱について補足しておく。コンテンツIDとスクランブル鍵K sの送出に関しては、コンテンツをリアルタイムに視聴する場合と同様の方法で配信される。一方、コンテンツ鍵K cは、コンテンツ、コンテンツIDおよびスクランブル鍵K sと同期（多重化）して送出させる必要はなく、コンテンツ受信装置5のユーザがコンテンツを再生させる時間より前に配信されればよい。例えば、予め、スクランブル化されたコンテンツとスクランブル鍵K sとを記憶部17aに記憶させておき、送信側のコンテンツ送信装置3の放送事業者が、記憶されたコンテンツの視聴を許可する場合に、そのコンテンツに対応するコンテンツ鍵が配信されることで、疑似ビデオオンデマンドが実現される。

【0131】（コンテンツ受信装置、セキュリティモジュール、不揮発性メモリの関係（構成））次に、図5を参照して、限定受信システム1におけるコンテンツ受信装置5とセキュリティモジュールSM3と不揮発性メモリFMとの関係を説明する。コンテンツ受信装置5は、受信したストリーム（多重暗号コンテンツ）からワーク鍵Kwとコンテンツ鍵K cを分離するKw・K c関連情報分離部13aと、暗号化コンテンツを記憶する記憶部17aと、スクランブル鍵K sを含む関連情報を分離するK s関連情報分離部13bと、コンテンツをデスクラン

ブルするコンテンツデスクランブル部15と、コンテンツ受信装置5とセキュリティモジュールSM3との通信を行うインターフェース（図示せず）と、記憶媒体（不揮発性メモリFMとは別途のものを取り扱う記憶媒体取扱手段17b（図5には図示せず））等から構成されている。

【0132】セキュリティモジュールSM3は、マスター鍵Kmを備え、4つの復号器（19a〜19d）と、1つの暗号化部21と、状況に応じて入力される複数の情報を制御する、3個のソフトウェアスイッチS/Wとを備えて構成されている。ソフトウェアスイッチS/W1に、入力される情報数は3個であり、この情報数に対応してa1〜a3のスイッチが備えられており、スイッチa1がリアルタイムにコンテンツを視聴する場合、スイッチa2が記憶再生視聴する場合、スイッチa3が既存放送の視聴の場合に対応している。また、ソフトウェアスイッチS/W2に入力される情報数は2個（b1、b2）であり、同様にソフトウェアスイッチS/W3に入力される情報数は2個（c1、c2）である。

【0133】不揮発性メモリFMは、コンテンツIDと共に、セキュリティモジュールSM3のマスター鍵によって再暗号化されたコンテンツ鍵K cを記憶し保持するものである。なお、この不揮発性メモリFMが請求項に記載した記憶媒体に相当するものである。

【0134】なお、この図5に示したコンテンツ受信装置5には、図示を省略した暗号化コンテンツ記憶手段と、関連情報入力手段と、スクランブル鍵出力手段と、暗号化コンテンツ復号手段とを備えている。なお、これらは、コンテンツ受信装置5の主制御部（図示せず）に展開している（起動している）プログラムである。

【0135】暗号化コンテンツ記憶手段は、記憶媒体取扱手段17bによって取り扱われる記憶媒体（不揮発性メモリFMとは別途に設けられる記憶媒体）に、スクランブル鍵K sで暗号化された暗号化コンテンツと、この暗号化コンテンツを識別するコンテンツ識別子を含むコンテンツに関する暗号化関連情報とを記憶させるものである。

【0136】関連情報入力手段は、暗号化コンテンツを再生する際に、当該暗号化コンテンツに対応する再暗号化コンテンツ鍵関連情報（固有暗号化コンテンツ鍵関連情報：固有鍵（グループ鍵K g）で暗号化されたもの）が記憶部17a、不揮発性メモリFMの少なくとも一方に記憶されている場合、当該再暗号化コンテンツ鍵関連情報（固有暗号化コンテンツ鍵関連情報）を記憶部17aまたは不揮発性メモリFMから読み出して、セキュリティモジュールSM3に入力すると共に、暗号化関連情報を入力するものである。

【0137】スクランブル鍵出力手段は、セキュリティモジュールSM3に設定されているマスター鍵Kmにより、再暗号化コンテンツ鍵関連情報（固有暗号化コンテ

ンツ鍵関連情報)を復号し、コンテンツ鍵Kcを得、このコンテンツ鍵Kcにより、暗号化関連情報を復号し、スクランブル鍵Ksを得、このスクランブル鍵Ksをコンテンツ受信装置5に出力させるものである。

【0138】暗号化コンテンツ復号手段は、このスクランブル鍵出力手段で出力されたスクランブル鍵Ksで、暗号化コンテンツを復号するものである。

【0139】(コンテンツ鍵が不揮発メモリに記憶された場合の暗号化コンテンツの再生)ソフトウェアスイッチS/W3を切り替えることで、暗号化器21で暗号化された再暗号化コンテンツ鍵Kcは、c1の場合は、記憶部17aに記憶され、c2の場合は、対応するコンテンツIDと共に、セキュリティモジュールSM3の外部に備えられる不揮発性メモリFMに記憶される。

【0140】記憶部17aに記憶されている暗号化コンテンツを再生するときに、記憶部17aにコンテンツ鍵Kcが暗号化コンテンツと併せて記憶されている場合、ソフトウェアスイッチS/W2をb1に切り替え、記憶部17aより読み出した再暗号化コンテンツ鍵KcをセキュリティモジュールSM3に入力し、復号器19cで復号し、コンテンツ鍵Kcを得る。このコンテンツ鍵Kcを用いて、Ks関連情報分離部13bで得られた、暗号化されたスクランブル鍵Ksを復号器19dで復号し、スクランブル鍵Ksを得る。このスクランブル鍵Ksを用いて、コンテンツデスクランブル部15で暗号化コンテンツをデスクランブルしコンテンツが得られる。

【0141】記憶部17aに記憶されている暗号化コンテンツIDと共に再暗号化コンテンツ鍵Kcが記憶されておらず、不揮発性メモリFMに記憶されている場合は、ソフトウェアスイッチS/W2をb2に切り替えて、再生させる暗号化コンテンツのコンテンツIDをKs関連情報分離部13bで取り出し、不揮発性メモリFMに入力する。

【0142】不揮発性メモリFMでは、入力されたコンテンツIDに対応する再暗号化コンテンツ鍵Kcが選択され、この再暗号化コンテンツ鍵KcがセキュリティモジュールSM3に入力される。セキュリティモジュールSM3では、入力された再暗号化コンテンツ鍵Kcがマスター鍵Kmにより復号器19cで復号され、コンテンツ鍵Kcが得られる。このコンテンツ鍵Kcを用いて、Ks関連情報分離部13bで得られる暗号化関連情報ECM-Kcを復号器19dで復号し、スクランブル鍵Ksを得て、コンテンツデスクランブル部15で、コンテンツが得られる。

【0143】次に、図6を参照して、不揮発性メモリFMがコンテンツ受信装置5に付属される場合の、関連情報のファイルフォーマットを説明する。コンテンツ鍵関連情報は、事業者ID、ワーク鍵ID、コンテンツID、コンテンツ鍵Kc、有効期限、記憶場所指定情報等から構成されている。記憶場所指定情報は、暗号化コン

テンツの送信側(放送局側)で再暗号化コンテンツ鍵Kcを暗号化コンテンツと共に、記憶部17aに記憶させるのか、それとも、不揮発性メモリFMに記憶させるのか等の選択をするための制御情報である。コンテンツ受信装置5のKw・Kc関連情報分離部13aで、コンテンツ鍵関連情報をセキュリティモジュールSM3に入力し、このコンテンツ鍵関連情報に記述されている記憶場所指定情報に基づいて、セキュリティモジュールSM3は、ソフトウェアスイッチS/W3を切り替えて、コンテンツ鍵Kcの記憶場所を制御する。

【0144】また、コンテンツ鍵関連情報に記述されている有効期限は、コンテンツ鍵Kcの有効期限を示すものであり、この有効期限内では、コンテンツ鍵Kcは有効とされる。なお、この有効期限を過ぎたコンテンツ鍵Kcは無効となる。また、有効期限の情報は、再暗号化コンテンツ鍵と併せて記憶部17aや不揮発性メモリFM内に記憶される。つまり、セキュリティモジュールSM3の復号器19cで、再暗号化コンテンツ鍵Kcを復号する際に、有効期限に基づいて、当該復号器19cが制御され、有効期限内であれば、再暗号化コンテンツ鍵Kcの復号が行われる。

【0145】図7に不揮発性メモリFMの記憶フォーマットを示す。不揮発性メモリFMでは、コンテンツID、コンテンツ鍵Kc(再暗号化コンテンツ鍵Kc)、このコンテンツ鍵Kcを記憶した記憶日時、およびコンテンツ鍵Kcの有効期限(有効期限情報)等が関係付けられて記憶されて管理されている。

【0146】再暗号化コンテンツ鍵Kcを不揮発性メモリFMに記憶させる場合、不揮発性メモリFMの記憶容量を越えた場合には、記憶日時が参照され、記憶日時が古い順に再暗号化コンテンツ鍵Kc、この再暗号化コンテンツ鍵Kcに対応するコンテンツID、記憶日時、有効期限が削除される。また、不揮発性メモリFM内の有効期限を参照して、記憶容量に拘わらず、有効期限が過ぎている再暗号化コンテンツ鍵Kc、この再暗号化コンテンツ鍵Kcに対応するコンテンツID、記憶日時、有効期限を削除する等の方法がある。

【0147】(コンテンツ鍵入手する際のシーケンスチャート)図8にコンテンツ鍵Kcを入手する際のシーケンスチャートを示す。まず、再生する暗号化コンテンツと併せて再暗号化コンテンツ鍵Kcが記憶部17aにあるかどうか判断される(S1)。記憶部17aに記憶されていると判断された場合には、その再暗号化コンテンツ鍵Kcが用いられる。再暗号化コンテンツ鍵Kcがないと判断された場合には、暗号化コンテンツのコンテンツIDをセキュリティモジュールSM3に入力し、セキュリティモジュールSM3または不揮発性メモリFM内に、対象となるコンテンツ鍵Kc(再暗号化コンテンツ鍵Kc)が記憶されているか確認される。セキュリ

象となるコンテンツ鍵Kc(再暗号化コンテンツ鍵Kc)が確認された場合は、確認された保持されているコンテンツ鍵Kcが用いられる。

【0148】対象となるコンテンツ鍵Kcが、コンテンツ受信装置5、セキュリティモジュールSM3、不揮発性メモリFMのいずれにも存在しない場合、送信側(放送局)に備えられているコンテンツ送信装置3に対して、コンテンツ鍵Kcの送付を、インターネットや公衆の通信回線網を介して要求する。この場合、カードIDおよびコンテンツIDをコンテンツ送信装置3に送信する(S2)。なお、コンテンツ鍵Kcの送付を要求する際に、コンテンツIDをマスター鍵Kmで暗号化しておけば、コンテンツ送信装置3側で送信元の確認ができる。

【0149】コンテンツ鍵Kcの送付の要求を受信したコンテンツ送信装置3には、マスター鍵KmおよびカードIDを対応させて、マスター鍵Kmを管理しているマスター鍵データベースと、コンテンツ鍵KcおよびコンテンツIDを対応させて、コンテンツ鍵Kcを管理しているコンテンツ鍵データベースが備えられている。そして、受信したカードIDに対応するマスター鍵Kmをマスター鍵データベースの中から選択する(S3)。選択されたマスター鍵Kmを用いて、受信した、暗号化されているコンテンツIDを復号し、コンテンツIDを得る(S4)。

【0150】得られたコンテンツIDに対応するコンテンツ鍵Kcをコンテンツ鍵データベースより選択する(S5)。そして、通信回線網を介してコンテンツ鍵Kcを配信する場合には、選択したマスター鍵Kmを用いて、このコンテンツ鍵Kcが暗号化され、暗号化コンテンツ鍵Kcとしてコンテンツ受信装置5に送出される(S6)。コンテンツ受信装置5では、受信した暗号化コンテンツ鍵Kcをマスター鍵Kmで復号し、暗号化コンテンツの再生に利用する(S7)。

【0151】S5の後、放送波を用いて、コンテンツ鍵Kcを配信する場合にも、選択したマスター鍵Kmを用いて、このコンテンツ鍵Kcが暗号化され、EMM(Kc配布用、図8参照)として配信(放送)される。なお、このEMM(Kc配布用)には、事業者ID、カードID、コンテンツID、コンテンツ鍵Kc、有効期限、記憶場所指定情報が含まれている。

【0152】(グループ鍵を用いた場合の限定受信システム)ここまでは、コンテンツ鍵KcがセキュリティモジュールSM1〜SM3内のマスター鍵Kmによって暗号化されると共に、暗号化コンテンツが記憶部17aや不揮発性メモリFM(記憶媒体)に記憶される場合を説明した。ここでは、セキュリティモジュール内に備えられているマスター鍵Kmで暗号化するのではなく、グループ鍵Kgを用いて暗号化する場合を述べる。

【0153】グループ鍵Kgは、複数のコンテンツ受信

装置5間で共有される鍵であり、セキュリティモジュール配布時に、予め、グループ鍵の識別子であるグループ鍵IDと対応させて、当該セキュリティモジュール内部に記憶されているものである。なお、グループ鍵Kgは請求項に記載したグループ分けされた後の固有鍵に相当するものである。

【0154】図5を参照して、グループ鍵Kgが用いられた場合のコンテンツ受信装置5を説明する。暗号化コンテンツを記憶するときにKw・Kc関連情報(図13aでコンテンツ鍵関連情報が抽出され、このコンテンツ鍵関連情報(暗号化されているコンテンツ鍵Kcを含む)がセキュリティモジュールSM3に入力される。セキュリティモジュールSM3では、入力された、暗号化されているコンテンツ鍵を復号器19cでワーク鍵Kwを用いて復号し、復号されたコンテンツ鍵Kcを暗号化器21に入力し、この暗号化器21でグループ鍵Kgを用いて再暗号化し、記憶部17aや、不揮発性メモリFMにコンテンツIDと対応させて記憶させる。なお、グループ鍵Kgを用いて再暗号化したコンテンツ鍵Kcが請求項に記載した固有暗号化コンテンツ鍵関連情報に相当する。

【0155】暗号化コンテンツを再生するときに、グループ鍵Kgで暗号化されているコンテンツ鍵Kcを、記憶部17aまたは不揮発性メモリFMから取り出し、セキュリティモジュールSM3に入力する。セキュリティモジュールSM3では、入力された、暗号化されているコンテンツ鍵Kcを復号器19cに入力し、グループ鍵Kgで復号し、コンテンツ鍵Kcを得て、このコンテンツ鍵KcがスクランブルKsの復号の際に用いられる。

【0156】ここで補足しておく、マスター鍵KmはセキュリティモジュールSM2に割り当てられている鍵であり、書き換えることの不可能な鍵である。それに対し、グループ鍵Kgは書き換えることが可能な鍵である。

【0157】(複数台のコンテンツ受信装置間での暗号化コンテンツの取扱)次に、複数台(2台)のコンテンツ受信装置5(5A、5B、図示せず)間で、一方のコンテンツ受信装置5Bで受信した暗号化コンテンツをDV等のリムーバブルメディアに記憶させた後、他方のコンテンツ受信装置5Aで再生する場合について説明する。

【0158】コンテンツ受信装置5Bでグループ鍵Kg b(コンテンツ受信装置5BのセキュリティモジュールSM3B(図示せず)に割り当てられているグループ鍵)を用いて記憶した暗号化コンテンツを、リムーバブルメディア等に記憶させ、このリムーバブルメディアをコンテンツ受信装置5Aによって取り扱って、記憶されている暗号化コンテンツを再生する場合を想定する。

【0159】コンテンツ受信装置5AのセキュリティモジュールSM3A(図示せず)内には、グループ鍵Kg

41

a (コンテンツ受信装置5AのセキュリティモジュールSM3A(図示せず)に割り当てられているグループ鍵)がある。ところが、コンテンツ受信装置5Bで記憶された暗号化コンテンツを、コンテンツ受信装置5Aで再生しようと試みても、グループ鍵Kgaでは、グループ鍵Kgbで暗号化されたコンテンツ鍵Kcを復号することはできないため、暗号化コンテンツを再生することはできない。そこで、コンテンツ受信装置5BのセキュリティモジュールSM3B(図示せず)に設定されているグループ鍵Kgbを、コンテンツ受信装置5AのセキュリティモジュールSM3Aに記憶させる手法について、図11を参照して、説明する。

【0160】まず、コンテンツ受信装置5Bを操作して、表示手段(図示せず)にセキュリティモジュールSM3BのカードIDbを表示させるインターフェース(図示せず)等を用いて、コンテンツ受信装置5BのカードIDbを調べる(S11)。次に、コンテンツ受信装置5Aを操作して、調べたカードIDbを、このコンテンツ受信装置5AのセキュリティモジュールSM3Aに入力し、入力されたカードIDbをコンテンツ受信装置5AのセキュリティモジュールSM3AのカードIDaとを、送信側(放送事業者)のコンテンツ送信装置3に送出する(S12)。

【0161】コンテンツ送信装置3には、記憶部17aにカードIDdと対応させてマスター鍵Kmおよびグループ鍵Kgを管理しているマスター鍵・グループ鍵データベースが備えられている。そして、コンテンツ送信装置3では、マスター鍵・グループ鍵データベースより、受信したカードIDaに対応するマスター鍵Kmaが選択される(S13)。そしてまた、マスター鍵・グループ鍵データベースより、受信したカードIDbに対応するグループ鍵Kgbを選択する(S14)。

【0162】通信回線を用いてグループ鍵Kgbを配信する場合は、マスター鍵Kmaを用いて、グループ鍵Kgbを暗号化し、コンテンツ受信装置5Aに送出する(S15)。コンテンツ受信装置5Aでは、セキュリティモジュールSM3A内のマスター鍵Kmaを用いて復号し、グループ鍵Kgbを得て、保持される(S16)。

【0163】放送波を用いてグループ鍵Kgbを配信する場合は、マスター鍵Kmaを用いて、グループ鍵Kgbを暗号化し、図6に示すEMM(Kg配布用)として配信する。なお、EMM(Kg配布用)は、事業者ID、カードID、更新番号、有効期限、グループ鍵ID、グループ鍵Kgから構成されている。そして、コンテンツ送信装置3は、カードIDaに対応させて、グループ鍵Kgbをマスター鍵・グループ鍵データベースに保存する(S17)。

【0164】この実施の形態では、以下の効果を奏す。まず、コンテンツ送信装置3では、送信されるコンテ

42

ツが経過時間と共に変更されるスクランブル鍵Ksによって暗号化され、暗号化コンテンツとされる。そして、スクランブル鍵Ksもコンテンツ毎に設けられたコンテンツ鍵Kcによって、コンテンツに関する関連情報と共に、暗号化され、暗号化関連情報とされる。また、コンテンツ鍵Kcもコンテンツの継続時間よりも長時間にわたり保持されるワーク鍵Kwによって、コンテンツ鍵に関する関連情報と共に、暗号化され、暗号化コンテンツ鍵関連情報とされる。さらに、ワーク鍵も受信側に共通に備えられたマスター鍵Kmによって、ワーク鍵Kwに関する関連情報と共に、暗号化され、暗号化ワーク鍵関連情報とされる。その後、暗号化されたこれらの情報が多重化され、送信される。

【0165】そして、コンテンツ受信装置5では、まず、送信側で多重された多重暗号コンテンツが、分離部13によって、受信される。そして、受信された多重暗号コンテンツは、この分離部13によって、暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報に分離される。その後、コンテンツデスクランブル部15(15a~15d)によって、マスター鍵により暗号化ワーク鍵関連情報が復号され、ワーク鍵が得られ、このワーク鍵により暗号化コンテンツ鍵関連情報が復号され、コンテンツ鍵が得られ、このコンテンツにより暗号化関連情報が復号され、スクランブル鍵が得られ、このスクランブル鍵により暗号化コンテンツが復号され、コンテンツが得られる。

【0166】このため、コンテンツ単位で、スクランブル鍵Ksを用いてスクランブル、デスクランブルしており、さらにこのスクランブル鍵Ksをコンテンツ鍵Kcで暗号化しているため、スクランブルされたコンテンツをデスクランブルする際の効率性が、このコンテンツ鍵Kcによって向上され、さらに、ワーク鍵Kwによってデスクランブルする際の暗号鍵の管理が容易に行うことができる。さらに、有料のコンテンツを視聴した場合の受信料の徴収が容易かつ確実に行える。

【0167】コンテンツ鍵関連情報記憶指定手段によって、受信側でコンテンツ鍵関連情報を保持する場所が、セキュリティモジュールSM、記憶部17a、不揮発性メモリMのいずれかに指定される。コンテンツ鍵が暗号化されて保持されているので、暗号化コンテンツを容易に復号できず、コンテンツの著作権を保護することができる。

【0168】コンテンツ単位で暗号化、復号を制御するため、従来の3階層(スクランブル鍵Ks、ワーク鍵Kw、マスター鍵Km)の鍵構造を4階層(コンテンツ鍵Kcを付加)の鍵構造で、制御することにより、ファイナル等の固定の暗号鍵ではなく、経過時間と共に変更される鍵(スクランブル鍵Ks、ワーク鍵Kw)を併用して、暗号化された暗号化コンテンツの不正受信に対する安全性が確保できる。

【0169】コンテンツ単位で暗号化、復号することにより、コンテンツ受信装置5において、保有されるべき暗号鍵（暗号キー）、つまり、コンテンツ鍵Kcの数が大幅に増加することに対して、セキュリティモジュールSM内部だけではなく、コンテンツ受信装置5の記憶部17aに再暗号化して記憶できる構成としたので、安全性を損なうことなく、コンテンツ鍵Kcが保存できる。

【0170】コンテンツ単位で暗号化することによる多量の鍵情報（暗号化関連情報、コンテンツ鍵関連情報、ワーク鍵関連情報）をコンテンツ受信装置5に個別に送信することなく、コンテンツ受信装置5共通の鍵（マスター鍵Km）で暗号化して送信することにより、データ伝送容量の負担を低減することができる。

【0171】記憶媒体（不揮発性メモリFM）に記憶される際には、コンテンツは暗号化されており、正規のセキュリティモジュールSMとコンテンツ受信装置5との組み合わせを所有していないコンテンツを視聴することができず、不正受信に対する安全性を確保することができる。

【0172】記憶媒体（不揮発性メモリFM）がコピーされても、セキュリティモジュールSMのコピーができないので、記憶媒体とセキュリティモジュールSMの組み合わせを所有していないとコンテンツをデスクランブルできず、コンテンツの著作権を保護することができる。

【0173】コンテンツ受信装置5間で、セキュリティモジュールSMのカードIDを共有できる場合には、私的利用の範囲として、使用しているコンテンツ受信装置5とセキュリティモジュールSMと交換するなどの相互使用が可能となる。コンテンツ受信装置5、暗号化コンテンツを記憶させる記憶装置（記憶部17a、または外部の記憶装置）には、固有のIDや非公開の部分を特に備えることなく構成されているので、コンテンツ受信装置5等の受信装置を製造する製造業者が自由に製造できる。

【0174】以上、一実施形態に基づいて本発明を説明したが、本発明はこれに限定されるものではない。コンテンツ送信装置3、コンテンツ受信装置5の各構成の処理を、一般的なプログラム言語で記述したコンテンツ送信プログラム、コンテンツ受信プログラムとみなすことも可能である。この場合も、コンテンツ送信装置3、コンテンツ受信装置5で得られる効果と同様の効果が得られる。さらに、このプログラムを記憶媒体（フレキシブルディスク、CD-ROM等）に記憶し、流通させることも可能である。

【0175】

【発明の効果】請求項1記載の発明によれば、まず、送信されるコンテンツがスクランブル鍵によって暗号化され、暗号化コンテンツとされる。そして、スクランブル鍵もコンテンツ鍵によって、コンテンツに関する関連情

報と共に、暗号化され、暗号化関連情報とされる。また、マスター鍵によって、コンテンツ鍵に関する関連情報と共に、暗号化され、暗号化コンテンツ鍵関連情報とされる。その後、暗号化されたこれらの情報が多重暗号コンテンツとされ、送信される。このため、多重暗号コンテンツを受信側でデスクランブルする際にコンテンツ単位でされるので、従来のストリーム単位で行われる場合と比較してデスクランブルの効率が向上する。

【0176】請求項2記載の発明によれば、まず、送信されるコンテンツがスクランブル鍵によって暗号化され、暗号化コンテンツとされる。そして、スクランブル鍵もコンテンツ鍵によって、コンテンツに関する関連情報と共に、暗号化され、暗号化関連情報とされる。また、コンテンツ鍵もワーク鍵によって、コンテンツ鍵に関する関連情報と共に、暗号化され、暗号化コンテンツ鍵関連情報とされる。さらに、ワーク鍵もマスター鍵によって、ワーク鍵に関する関連情報と共に、暗号化され、暗号化ワーク鍵関連情報とされる。その後、暗号化されたこれらの情報が多重化され、送信される。このため、多重暗号コンテンツを受信側でデスクランブルする際にコンテンツ単位でされるので、従来のストリーム単位で行われる場合と比較してデスクランブルの効率が向上する。

【0177】請求項3記載の発明によれば、暗号化コンテンツが多重暗号コンテンツとして送信された後、暗号化コンテンツ鍵関連情報送信手段によって、暗号化コンテンツ鍵関連情報が別途送信されるので、暗号化コンテンツをデスクランブルする際に用いる暗号鍵（コンテンツ鍵）を、受信側で厳密に管理する必要性が低くなり、暗号鍵の管理が容易に行える。

【0178】請求項4記載の発明によれば、受信側にセキュリティモジュールが備えられた場合、このセキュリティモジュールがグループ分けされており、このグループ分けされたグループ毎に対応するワーク鍵が備えられている。このため、グループ毎に対応するワーク鍵によって、復号されるコンテンツ鍵の管理が容易に行える。

【0179】請求項5記載の発明によれば、コンテンツ鍵関連情報記憶指指定手段によって、受信側でコンテンツ鍵関連情報を保持する場所が、セキュリティモジュール、記憶手段、記憶媒体のいずれかに指定される。このため、セキュリティモジュール、記憶手段、記憶媒体のメモリ容量、重要度等に応じて、暗号鍵の管理場所を受信側で指定することができ、暗号鍵の管理が容易に行える。

【0180】請求項6記載の発明によれば、受信側で、暗号化コンテンツが再生されるときに、コンテンツ鍵関連情報利用指指定手段によって、当該暗号化コンテンツを復号するスクランブル鍵に対応するコンテンツ鍵を含むコンテンツ鍵関連情報が送信されている場合であっても、これを利用せずに、保持されているコンテンツ鍵関連

連情報しか利用できないように指定される。このため、暗号化コンテンツを復号するのに供されるコンテンツ鍵が指定されているので、コンテンツを不正受信したり、不正に利用したりすることが困難になり、コンテンツの著作権を保護することができる。

【0181】請求項7記載の発明によれば、受信側にセキュリティモジュールが備えられる際に、このセキュリティモジュールの内部に設定される固有鍵が、送信側の固有鍵設定用関連情報暗号化手段によって、マスター鍵により暗号化された暗号化固有鍵設定用関連情報とされ、送信される。このため、セキュリティモジュールに設定される固有鍵を送信側で自在に変更することができる。

【0182】請求項8記載の発明によれば、受信側の他のセキュリティモジュールに共通する固有鍵が設定されているので、この共通の固有鍵を利用すれば、一方のセキュリティモジュールに記憶されている情報（例えば、コンテンツ鍵関連情報）を、他方のセキュリティモジュールで出力させられる。このため、例えば、受信側で、セキュリティモジュールの識別子を複数受信装置間で共有できる場合には、私的利用の範囲として、使用している受信装置とセキュリティモジュールとを交換するなどの相互使用が可能となる。

【0183】請求項9記載の発明によれば、まず、送信側で多重された多重暗号コンテンツが、多重暗号コンテンツ受信手段によって受信され、受信された多重暗号コンテンツが多重暗号コンテンツ分離手段によって分離される。その後、多重暗号コンテンツ復号手段によって復号され、コンテンツが得られる。このため、多重暗号コンテンツをデスクランブルする際にコンテンツ単位でされるので、従来のストリーム単位で行われる場合と比較してデスクランブルの効率が向上する。

【0184】請求項10記載の発明によれば、まず、送信側で多重された多重暗号コンテンツが、多重暗号コンテンツ受信手段によって受信され、受信された多重暗号コンテンツは、多重暗号コンテンツ分離手段によって、暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報に分離される。その後、多重暗号コンテンツ復号手段によって、マスター鍵により暗号化ワーク鍵関連情報が復号され、ワーク鍵が得られ、このワーク鍵により暗号化コンテンツ鍵関連情報が復号され、コンテンツ鍵が得られる。このコンテンツにより暗号化関連情報が復号され、スクランブル鍵が得られ、このスクランブル鍵により暗号化コンテンツが復号され、コンテンツが得られる。このため、多重暗号コンテンツをデスクランブルする際にコンテンツ単位でされるので、従来のストリーム単位で行われる場合と比較してデスクランブルの効率が向上する。

【0185】請求項11記載の発明によれば、暗号化コンテンツ鍵関連情報が得られていない場合に、暗号化コンテンツ鍵関連情報要求手段によって、送信側にコンテ

ンツ鍵が含まれている暗号化コンテンツ鍵関連情報が要求されるので、受信側でコンテンツを再生する場合に、必要に応じてコンテンツ鍵を入力することができる。

【0186】請求項12記載の発明によれば、コンテンツ鍵関連情報記憶手段によって、復号後のコンテンツ鍵関連情報とコンテンツを識別するコンテンツ識別子とが、マスター鍵が設定されたセキュリティモジュールに記憶されるので、コンテンツ鍵の保護がなされ、ひいてはコンテンツの著作権の保護が行える。

10 【0187】請求項13記載の発明によれば、コンテンツ鍵関連情報記憶手段によって、復号後のコンテンツ鍵関連情報とコンテンツを識別するコンテンツ識別子とが、マスター鍵および固有鍵が設定されたセキュリティモジュールに記憶されるので、コンテンツ鍵の保護がなされ、ひいてはコンテンツの著作権の保護が行える。

【0188】請求項14記載の発明によれば、マスター鍵および固有鍵が設定されるセキュリティモジュールにおいて、少なくとも1つの固有鍵が、他のセキュリティモジュールと共通に設定されており、この共通の固有鍵を利用すれば、一方のセキュリティモジュールに記憶されている情報（例えば、コンテンツ鍵関連情報）を、他方のセキュリティモジュールで出力させられる。このため、例えば、セキュリティモジュールの識別子を複数受信装置間で共有できる場合には、私的利用の範囲として、使用している受信装置とセキュリティモジュールとを交換するなどの相互使用が可能となる。

【0189】請求項15記載の発明によれば、セキュリティモジュールの内部に固有鍵が設定されている場合に、暗号化固有鍵設定用関連情報受信手段によって、送信側でマスター鍵により暗号化された暗号化固有鍵設定用関連情報を受信し、暗号化固有鍵設定用関連情報復号手段によって、暗号化固有鍵設定用関連情報を復号し、固有鍵が得られる。このため、セキュリティモジュールに設定される固有鍵を送信側で自在に変更されるので、コンテンツの著作権の保護が行える。

【0190】請求項16記載の発明によれば、セキュリティモジュールのメモリ容量を越えた場合に、コンテンツ鍵関連情報削除手段によって、コンテンツ鍵関連情報が記憶された時間、送信側または受信側により設定された設定情報に基づいて、コンテンツ鍵関連情報が削除されるので、コンテンツ鍵の管理が容易に行える。

【0191】請求項17記載の発明によれば、セキュリティモジュールに記憶された復号後のコンテンツ鍵関連情報が、コンテンツ鍵関連情報出力記憶手段によって、出力され記憶されるので、コンテンツ鍵の管理が容易に行える。

【0192】請求項18記載の発明によれば、記憶手段のメモリ容量を越えた場合に、コンテンツ鍵関連情報削除手段によって、コンテンツ鍵関連情報が記憶された時間、送信側または受信側により設定された設定情報に基

づいて、コンテンツ鍵関連情報が削除されるので、コンテンツ鍵の管理が容易に行える。

【0193】請求項19記載の発明によれば、コンテンツ鍵関連情報再暗号化記憶手段によって、セキュリティモジュールに記憶されている復号後のコンテンツ鍵関連情報がマスター鍵により、再暗号化されて出力され、記憶されるので、コンテンツ鍵の保護がなされ、ひいてはコンテンツの著作権の保護が行える。

【0194】請求項20記載の発明によれば、記憶手段のメモリ容量を越えた場合に、再暗号化コンテンツ鍵関連情報削除手段によって、再暗号化コンテンツ鍵関連情報が記憶された時間、送信側または受信側により設定された設定情報に基づいて、再暗号化コンテンツ鍵関連情報が削除されるので、コンテンツ鍵の管理が容易に行える。

【0195】請求項21記載の発明によれば、コンテンツ鍵関連情報固有暗号化記憶手段によって、セキュリティモジュールに記憶されている復号後のコンテンツ鍵関連情報が固有鍵により、再暗号化されて、固有暗号化コンテンツ鍵関連情報として出力され、記憶されるので、コンテンツ鍵の保護がなされ、ひいてはコンテンツの著作権の保護が行える。

【0196】請求項22記載の発明によれば、記憶手段のメモリ容量を越えた場合に、固有暗号化コンテンツ鍵関連情報削除手段によって、固有暗号化コンテンツ鍵関連情報が記憶された時間、送信側または受信側により設定された設定情報に基づいて、固有暗号化コンテンツ鍵関連情報が削除されるので、コンテンツ鍵の管理が容易に行える。

【0197】請求項23記載の発明によれば、セキュリティモジュールに記憶された復号後のコンテンツ鍵関連情報が、記憶媒体取扱手段によって、マスター鍵により暗号化され再暗号化コンテンツ鍵関連情報とされ、暗号化コンテンツと共に、記憶媒体に記憶されるので、コンテンツ鍵の保護がなされ、ひいてはコンテンツの著作権の保護が行える。

【0198】請求項24記載の発明によれば、セキュリティモジュールに記憶された復号後のコンテンツ鍵関連情報が、記憶媒体取扱手段によって、固有鍵により暗号化され固有暗号化コンテンツ鍵関連情報とされ、暗号化コンテンツと共に、記憶媒体に記憶されるので、コンテンツ鍵の保護がなされ、ひいてはコンテンツの著作権の保護が行える。

【0199】請求項25記載の発明によれば、暗号化コンテンツ関連情報記憶手段によって、記憶媒体に暗号化コンテンツとこの暗号化コンテンツに対応する暗号化関連情報とが記憶され、関連情報入力手段によって、記憶手段または記憶媒体に記憶されている再暗号化コンテンツ鍵関連情報を、セキュリティモジュールに入力し、スクランブル鍵出力手段によって、再暗号化コンテンツ鍵

関連情報が復号され、コンテンツ鍵が得られ、このコンテンツ鍵により、暗号化関連情報が復号され、スクランブル鍵が得られ、暗号化コンテンツ復号手段によって、暗号化コンテンツが復号される。このため、暗号化コンテンツを再生する場合に、コンテンツ鍵が複雑なプロセスを経なければ、コンテンツ鍵が入手できないので、コンテンツの著作権の保護が行える。

【0200】請求項26記載の発明によれば、暗号化コンテンツ関連情報記憶手段によって、記憶媒体に暗号化コンテンツとこの暗号化コンテンツに対応する暗号化関連情報とが記憶され、関連情報入力手段によって、記憶手段または記憶媒体に記憶されている固有暗号化コンテンツ鍵関連情報を、セキュリティモジュールに入力し、スクランブル鍵出力手段によって、固有暗号化コンテンツ鍵関連情報が復号され、コンテンツ鍵が得られ、このコンテンツ鍵により、暗号化関連情報が復号され、スクランブル鍵が得られ、暗号化コンテンツ復号手段によって、暗号化コンテンツが復号される。このため、暗号化コンテンツを再生する場合に、コンテンツ鍵が複雑なプロセスを経なければ、コンテンツ鍵が入手できないので、コンテンツの著作権の保護が行える。

【0201】請求項27記載の発明によれば、コンテンツ鍵不記憶手段によって、暗号化コンテンツを記憶しない場合、この暗号化コンテンツに対応するコンテンツ鍵、すなわち、暗号化コンテンツ鍵関連情報が記憶されないの、暗号化コンテンツを別途記憶しておいても再生することができず、当該コンテンツの著作権の保護が行える。

【0202】請求項28記載の発明によれば、コンテンツ鍵切替手段によって、暗号化関連情報をコンテンツ鍵で復号するタイミングがコンテンツの送信開始時刻、終了時刻に基づいて、切り替えられるので、受信側で、コンテンツ鍵が得られていれば、コンテンツの送信開始時刻から終了時刻まで暗号化関連情報を復号することができる。

【0203】請求項29記載の発明によれば、まず、送信されるコンテンツがスクランブル鍵によって暗号化され、暗号化コンテンツとされる。そして、スクランブル鍵もコンテンツ鍵によって、コンテンツに関する関連情報と共に、暗号化され、暗号化関連情報とされる。また、コンテンツ鍵もワーク鍵によって、コンテンツ鍵に関する関連情報と共に、暗号化され、暗号化コンテンツ鍵関連情報とされる。さらに、ワーク鍵もマスター鍵によって、ワーク鍵に関する関連情報と共に、暗号化され、暗号化ワーク鍵関連情報とされる。その後、暗号化されたこれらの情報が多重化され、送信される。このため、多重暗号化コンテンツを受信側でデスクランブルする際にコンテンツ単位でされるので、従来のストリーム単位で行われる場合と比較してデスクランブルの効率性が向上する。

【0204】請求項30記載の発明によれば、まず、送信側で多重された多重暗号コンテンツが、多重暗号コンテンツ受信手段によって受信され、受信された多重暗号コンテンツは、多重暗号コンテンツ分離手段によって、暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報に分離される。その後、多重暗号コンテンツ復号手段によって、マスター鍵により暗号化ワーク鍵関連情報が復号され、ワーク鍵が得られ、このワーク鍵により暗号化コンテンツ鍵関連情報が復号され、コンテンツ鍵が得られ、このコンテンツにより暗号化関連情報が復号され、スクランブル鍵が得られ、このスクランブル鍵により暗号化コンテンツが復号され、コンテンツが得られる。このため、多重暗号コンテンツをデスクランブルする際にコンテンツ単位でされるので、従来のストリーム単位で行われる場合と比較してデスクランブルの効率が向上する。

【図面の簡単な説明】

【図1】本発明による一実施の形態である限定受信システム（コンテンツ送信装置、コンテンツ受信装置）のブロック図である。

【図2】スクランブル鍵Ks、コンテンツ鍵Kc、ワーク鍵Kwをバケット化する際のファイルフォーマットを説明した図である。

【図3】限定受信システムにおけるコンテンツ受信装置とセキュリティモジュールとのブロック図である。

【図4】コンテンツ受信装置に入力されるストリーム（多重暗号コンテンツ）に対する、スクランブル鍵、コンテンツ鍵、ワーク鍵の時間変化を説明した図である。

【図5】グループ鍵が用いられた場合のコンテンツ受信装置を説明したブロック図である。

【図6】コンテンツ鍵関連情報、ワーク鍵関連情報等のファイルフォーマットを説明した図である。

【図7】不揮発性メモリの記憶フォーマットを説明した図である。

* 【図8】コンテンツ鍵を入手する際のシーケンスチャートである。

【図9】コンテンツ受信装置およびセキュリティモジュールを用いて、既存のBSデジタル放送を記憶後、視聴する場合のブロック図である。

【図10】コンテンツ受信装置およびセキュリティモジュールを用いて、既存のBSデジタル放送を記憶後、ワーク鍵利用して視聴する場合のブロック図である。

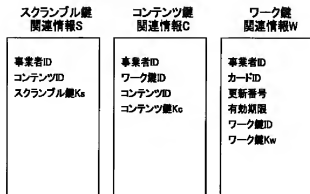
【図11】グループ鍵を入手する際のシーケンスチャートである。

【図12】従来の、限定受信システムのブロック図である。

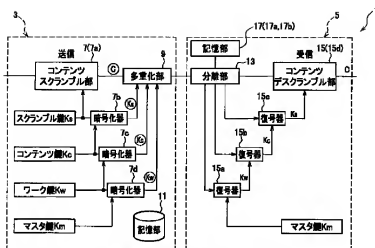
【符号の説明】

- 1 限定受信システム
- 3 コンテンツ送信装置
- 5 コンテンツ受信装置
- 7 コンテンツスクランブル部
- 9 多重化部
- 11 記憶部
- 13 分離部
- 15 コンテンツデスクランブル部
- 17 記憶部
- 15a、15b、15c、15d、19a、19b、19c、19d 復号器
- 7a、7b、7c、7d、21 暗号化器
- Ks スクリブル鍵
- Kc コンテンツ鍵
- Kw ワーク鍵
- Km マスター鍵
- 30 Kg グループ鍵（固有鍵）
- SM、SM1、SM2、SM3 セキュリティモジュール
- FM 不揮発性メモリ

【図2】

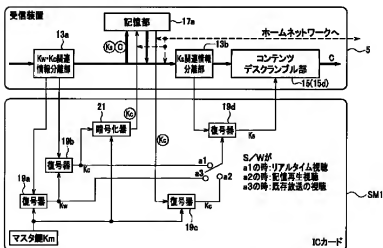


【図1】

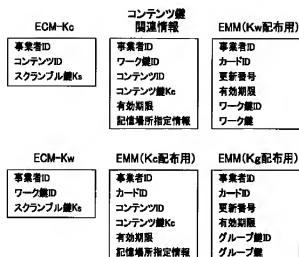


※○で囲まれた記号は、暗号化されていることを示している。

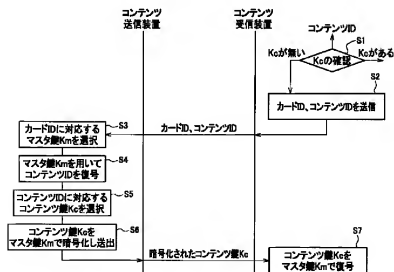
【図3】



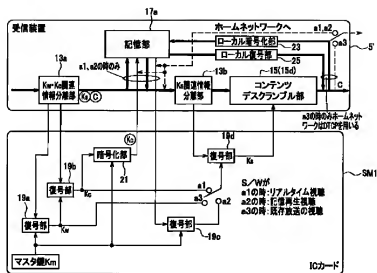
【図6】



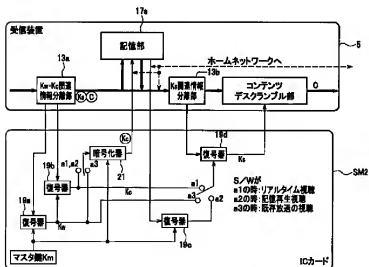
【図8】



【図9】



【図10】



The flowchart illustrates the process of matching card IDs between a transmitting device (送信装置) and a receiving device A (受信装置A). The process is divided into two main paths based on whether the receiving device A has a group key K_g in common with the transmitting device.

Left Path (S13-S17): This path is executed when the receiving device A does not have a common group key. It involves:

- S13:** Selecting a master key K_{ma} corresponding to the card ID ID_a of the transmitting device.
- S14:** Selecting a group key K_g corresponding to the card ID ID_b of the receiving device A.
- S15:** Using the master key K_{ma} to encode the group key K_g and outputting the encoded group key.
- S17:** Matching the card ID ID_a and storing the group key K_g.

Right Path (S11-S16): This path is executed when the receiving device A has a common group key K_g with the transmitting device. It involves:

- S11:** Searching for the card ID ID_b of the receiving device A.
- S12:** Outputting the card ID ID_a of the transmitting device and the card ID ID_b of the receiving device A.
- S16:** Encoding the group key K_g using the received card IDs and storing the encoded group key in the IC card.

Central Labels: The flowchart is divided into two sections by a vertical line. The left section is labeled "送信装置" (Transmitting Device) and the right section is labeled "受信装置A" (Receiving Device A). The central flow is labeled "受信装置AのカードIDa 受信装置BのカードIDb" (Card ID a of Receiving Device A, Card ID b of Receiving Device B).

Figure 1 is a block diagram of a digital audio transmission system. The system is divided into a transmitter (送信) and a receiver (受信).
 In the transmitter:
 - '録音・音声データ' (Recording/Audio Data) is input to the 'スクランブル部' (Scrambling Unit).
 - The 'スクランブル部' outputs 'スクランブルデータ' (Scrambled Data) to the '多重化部' (Multiplexing Unit).
 - The '多重化部' also receives 'ECM' (Entitlement Control Message) and 'EVM' (Entitlement Verification Message) and outputs to the '分離部' (Demultiplexing Unit).
 - The '分離部' outputs to the 'デスクランブル部' (Descrambling Unit).
 - The 'デスクランブル部' outputs '復号データ' (Decoded Data) to the '配信装置' (Distribution Device).
 In the receiver:
 - The 'ワーク鍵Kw' (Work Key) and 'マスク鍵Km' (Mask Key) are inputs to the '暗号化器' (Encryption Unit).
 - The '暗号化器' outputs to the '復号器' (Decryption Unit).
 - The '復号器' also receives 'Ks' (Scrambling Key) from the '分離部' and 'Kd' (Decryption Key) from the '配信装置'.

Fターム(参考) 5B017 AA03 BA07 CA07 CA16
5C025 DA01 DA10
5C052 AA01 AB02 DD04
5J104 AA01 AA16 EA07 EA17 NA02
PA05

(72)発明者 難波 誠一
東京都世田谷区砧一丁目10番11号 日本放
送協会放送技術研究所内